PROTOCOLO DE GOBIERNO Y GESTIÓN DE IDENTIDADES DIGITALES Y DE CONTROL DE ACCESO EN EL CONTEXTO DE UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR

CARLOS ADOLFO MARTÍNEZ TRONCOSO CERA

FUNDACIÓN UNIVERSIDAD DEL NORTE
DIVISIÓN DE INGENIERÍAS
MAESTRÍA EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA
BARRANQUILLA
2018

PROTOCOLO DE GOBIERNO Y GESTIÓN DE IDENTIDADES DIGITALES Y DE CONTROL DE ACCESO EN EL CONTEXTO DE UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR

CARLOS ADOLFO MARTÍNEZ TRONCOSO CERA

Proyecto presentado como requisito para optar el título de Magíster en Gobierno de Tecnología Informática.

Tutor:
Ing. WILSON NIETO BERNAL
Doctor en Ciencias de la computación
ULPCG España

FUNDACIÓN UNIVERSIDAD DEL NORTE
DIVISIÓN DE INGENIERÍAS
MAESTRÍA EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA
BARRANQUILLA
2018

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Firma presidente del Jurado

_____

Firma Jurado 1

_____

Firma Jurado 2

TABLA DE CONTENIDO

AGRADECIMIENTOS

A mis padres Lilia y Rafael quienes siempre han creído en el poder de la educación y el conocimiento,
a mi esposa Lida, y mis hijos Daniel y Gabriel, quienes son mi motor y soporte,
a mis hermanos y familiares quienes siempre han creído en mí,
a la Universidad del Norte por haberme concedido la beca, en especial a John Flórez y Emma Galiano por su apoyo,
a los docentes de la Universidad en especial a Wilson Nieto por su guía,
a mis compañeros de estudio por su acompañamiento y enseñanzas,
a mis compañeros de la Universidad por su apoyo y buenos deseos.

Dedicado a la memoria de mis abuelos Lilia, Maximiliano, Carlos y Margot, y de mis tíos César y Emilio.

1. INTRODUCCIÓN

En la actualidad el uso de herramientas TIC para apoyar los procesos básicos de una institución de educación superior es fundamental. Por ello es común encontrar tanto en la gestión administrativa como en el ejercicio de la formación, el uso de variadas herramientas informáticas y de ambientes virtuales donde intervienen estudiantes, docentes, empleados, egresados y proveedores, entre otros. Todo esto implica que en los diferentes sistemas y aplicativos, se generen identidades digitales o electrónicas (comúnmente llamadas cuentas de usuario) para cada entidad (persona, aplicativo, dispositivo, etc) que opera o participa de estos.

Como es de esperarse, esto conlleva la necesidad de establecer controles y mecanismos para determinar qué o quién y de qué forma, accede no solo a la información, sino también a otros recursos como dispositivos o lugares. Por ello, es esencial contar con estructuras y métodos de gobierno corporativo y de TI que permitan gestionar el acceso a estos.

Es en este contexto donde surge el concepto de gobierno y gestión de identidades digitales y de control de acceso, que consiste en una combinación de soluciones que permiten gestionar el ciclo de vida de las identidades y controlar el acceso a los diferentes recursos, con el objetivo de mitigar riesgos, reducir costos y permitir que las organizaciones evolucionen de manera flexible y segura.

Esta investigación revisará en primera medida, estándares de gobierno y gestión de Tecnología Informática con el fin de proponer un protocolo novedoso concerniente a la gestión de identidades digitales y de control de acceso que aplique a las necesidades de las instituciones de educación superior, y seguidamente mostrará el uso de este mediante un caso de estudio aplicado a la Universidad del Norte.

De los capítulos 1 al 4 encontrará la problemática que motiva el desarrollo de esta investigación junto a la justificación de esta, los objetivos planteados y el alcance de la misma. En el capítulo 5 nos introduciremos en el marco conceptual requerido para este proyecto (Gobierno, Gobierno TI, Gobierno y Gestión de Identidades, Gestión de Identidades) junto a una revisión del estado del arte en el capítulo 6. En el capítulo 7 se detalla el protocolo propuesto y en el 8 el resultado de aplicarlo en la Universidad del Norte. Finalmente se emiten las conclusiones del trabajo realizado.

2. PROBLEMÁTICA Y JUSTIFICACIÓN

La información es uno de los activos más preciados en cualquier organización y por ello se hace necesario establecer controles de acceso adecuados a esta con el fin de determinar, que la persona correcta, tenga el acceso correcto, en el momento correcto. De igual forma se hace necesario para el acceso físico a sitios o lugares. Esto también puede extenderse al software o a dispositivos.

Para el caso del sector de las Instituciones de Educación Superior (IES), donde los requerimientos giran alrededor del apoyo estratégico a las funciones de docencia, investigación, extensión y proyección social, la gestión de la seguridad de la información de sus procesos es fundamental. Aunque las instituciones de educación no están obligadas a implementar un Sistema de Gestión de Seguridad de la Información, si es deseable, por no decir que obligatorio, el definir una serie de buenas prácticas en este sentido para los diferentes procesos de la organización y con esto, implementar controles y mecanismos de seguridad.

Si bien el área administrativa de una Universidad es semejante al de otras compañías, en lo que respecta a su área académica, si es diferente, ya que los profesores necesitan tener bien custodiada la información de sus investigaciones, pero a la vez tener parte de ésta altamente disponible para compartirla con sus estudiantes o pares académicos. Cuando están en un salón de clases necesitan acceder a la información que tienen en su oficina o laboratorio. Los estudiantes requieren acceso fácil, pero seguro, desde las bibliotecas, salones y áreas de estudio, además de que en ocasiones pueden hacer sus prácticas profesionales en la misma entidad educativa y por lo tanto, tener además el rol de empleado. Con respecto a los egresados se tiene que en ocasiones se les ofrecen algunos servicios y facilidades de acceso al campus universitario.

Por lo antes expuesto, el reto de las universidades está en mantener segura su información, dispositivos e instalaciones, en un ambiente libre, de constante movimiento y cambio.

Por ello el no contar con un protocolo o conjunto de políticas y mecanismos que establezcan claramente quien, cuando y como se puede acceder a la información, a un dispositivo o a un lugar, puede conllevar a situaciones tales como un empleado que ha tenido varios cambios de cargo, mantenga los permisos de sus anteriores posiciones, un aplicativo en que los usuarios tienen acceso no controlado, un exfuncionario del área de Tesorería que siga pudiendo acceder a las instalaciones físicas donde se almacenan títulos valores, o un estudiante que mantiene los permisos que se le asignaron cuando trabajó temporalmente en su universidad.

Lo anterior son solo ejemplos de los múltiples casos en que por la falta de un gobierno

de identidades digitales se podrían materializar riesgos tales como[1]:

- Acceso y publicación no autorizados de información sensible o privada.
- Modificación no autorizada de información.
- Indisponibilidad de la información.
- Afectación de la seguridad física de la organización y su comunidad debido al acceso de personal no autorizado a sus instalaciones o a sitios restringidos.
- Sobrecarga de solicitudes al personal técnico por no tener una política de acceso definida.
- Imposibilidad de atender requerimientos de auditoría o de trazabilidad de transacciones o accesos.
- Incumplimiento de leyes y regulaciones.

Una solución para lo antes expuesto consiste en implementar un sistema de gestión de identidades el cual podemos definir como "un sistema integrado de procesos, políticas y tecnologías que permiten a las organizaciones facilitar y controlar el acceso de los usuarios a sus recursos y aplicaciones, permitiendo a la vez proteger su información, de usuarios no autorizados"[2].

Implementar un protocolo de gobierno y gestión de identidades trae consigo que:

- Permite que todas las partes interesadas tengan los accesos necesarios para el desarrollo de sus funciones.
- Establece los controles adecuados.
- Se alinea a los procesos de la compañía.
- Mantiene la disponibilidad de la información.
- Facilita la trazabilidad de los accesos y actividades más relevantes.

[1] The Institute of Internal Auditors. (2007). Identity and Access Management.

[2] Iglesias, Ignacio. (2014). Por qué implantar un sistema de gestión de identidad open source: WBSVision.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Diseñar un protocolo de Gobierno y Gestión de identidades digitales, en el contexto de una organización educativa con el objeto de mejorar las capacidades de control de acceso a sus recursos o aplicaciones.

3.2. OBJETIVOS ESPECÍFICOS

1. Elaborar un estado del arte conceptual de Gobierno y Gestión de TI y su aplicación en el contexto de las identidades digitales en organizaciones educativas.
2. Analizar los estándares o marcos de trabajo asociados con Gobierno y Gestión de identidades digitales.
3. Formular los procesos, controles para la implementación de un protocolo de Gobierno y Gestión de identidades digitales con fin el de desplegarlo en una organización académica de educación superior.
4. Proponer un plan de implementación para desplegar el protocolo desarrollado en una institución universitaria: caso de estudio Universidad del Norte.

4. ALCANCE

El alcance del proyecto está determinado por los siguientes entregables:

1. Definir un protocolo de gobierno y gestión de identidades digitales y de acceso en el contexto de una organización educativa.
2. Establecer el nivel de madurez para la Universidad del Norte con el protocolo planteado.
3. Definir una propuesta de plan de trabajo para aumentar el nivel de madurez de la Universidad del Norte. Dependiendo del nivel obtenido, se estarían generando varias propuestas para cada nivel según el caso.

Se tomarán como puntos de referencia, entre otros, los siguientes marcos y conjunto de buenas prácticas: COBIT 5, ITIL v3, ISO 27002.

Los procesos claves para lograr el objetivo propuesto son: Investigación, levantamiento de información, alineación de marcos y estándares, elaboración del protocolo, construcción de guía de implementación, evaluar la Universidad del Norte con respecto el protocolo realizado, propuesta de aplicación para la Universidad del Norte y cierre.

Es importante, además, hacer la salvedad que los conceptos y opiniones tratados y consignados en este trabajo no comprometen a ningún funcionario de una universidad ni a una universidad en particular, son de total autoría del creador de este documento y tienen como único objetivo el consolidar un trabajo académico, para cumplir con el requerimiento final de grado del programa de Maestría que se encuentra cursando.

5. MARCO TEÓRICO

5.1. GOBIERNO CORPORATIVO

Gobierno Corporativo es el conjunto de responsabilidades y prácticas ejercidas por el consejo y la dirección ejecutiva con el objetivo de proporcionar una dirección estratégica, para asegurar que los objetivos se alcanzan, que los riesgos se gestionan adecuadamente y verificar que los activos de la empresa se utilizan de una manera responsable[3].

Los aspectos claves en las que se centra el Gobierno Corporativo incluyen principalmente:

1. Funciones de la Junta Directiva y Ejecutivos.
2. Cumplimiento normativo
3. Derechos de los accionistas
4. Operación y Control del negocio
5. Contabilidad Financiera y Reportes
6. Gestión de riesgos.

5.2. GOBIERNO Y GESTIÓN DE TI

Se entiende por Gobierno TI (Tecnologías de la Información), el conjunto de acciones que realiza el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o de negocio[4].

Constituye una parte esencial del gobierno de la empresa en su conjunto y aglutina la estructura organizativa y directiva ya que esta unión necesaria para asegurar que las Tecnologías de la Información sean las que soporten y faciliten el desarrollo de los objetivos estratégicos definidos por la compañía...

La implantación de un sistema de Gobierno de las TI en una organización pasa por cuatro pasos fundamentales:

[3] IT-Governance Institute. (2009).

[4] Selig, Gad & Wilkinson, Jayne. (2008). Implementing IT Governance: A Practical Guide to Global Best Practices in IT Management.

1. Formar a los directivos y responsables TI en los principales conceptos del Gobierno de las TI.
2. Conocer y evaluar cuál es la situación inicial del Gobierno de las TI en su organización.
3. Definir cuál sería la situación deseable en relación con el Gobierno de las TI.
4. Redactar un Plan de Implantación del Gobierno de las TI que establezca las acciones a llevar a cabo para cubrir la distancia existente entre estas dos situaciones.[5].

Figura 1. Componentes del Gobierno de TI[6]

Según UST Global el marco en el cual se desenvuelve un buen Gobierno de TI es:

1. Alineación estratégica, la cual se centra en:
    a. Asegurar la conexión e integración del negocio con los planes de TI.
    b. Definir, mantener y validar las propuestas de valor de TI.
    c. Alinear las operaciones de TI con las de la empresa.
    d. Obtener mejor alineación que la competencia.

[5] Van Grembergen y De Haes. (2015). Enterprise Governance of Information Technology.
[6] Tomado de https://www.servicetonic.es/itil/introduccion-a-itil-v3/

2. Entrega de valor: Se refiere a ejecutar las propuestas de valor durante el ciclo de entrega, asegurando que TI entrega los beneficios relacionados con la estrategia del negocio, concentrándose en optimizar costos y proporcionar el valor intrínseco a la TI.

3. Gestión del Riesgo requiere:
    a. Cultura Organizacional por parte de la alta gerencia.
    b. Comprender y entender con total claridad la necesidad del cumplimiento de todos los requisitos requeridos.
    c. Transparencia y acción inmediata en el tratamiento de los riesgos.
    d. Trabajar en conjunto con todas las áreas para la adecuada gestión de riesgos en la organización.

4. Gestión de Recursos, se centra en:
    a. Organizar de manera óptima los recursos de TI de forma que los servicios que los requieran los obtengan en el lugar y momento necesarios.
    b. Alinear y priorizar servicios y productos existentes de TI que se requieren para apoyar las operaciones del negocio.
    c. Controlar y monitorear los servicios TI propios y de terceros.

5. Medición del Rendimiento, sigue y controla:
    a. La estrategia de la implantación.
    b. La estrategia de los proyectos.
    c. El uso de los recursos.
    d. El rendimiento de los procesos.
    e. La entrega de los servicios utilizando BSC.

Se deben tener claros los objetivos de negocio y estructurarlos de la mejor forma posible para que los procesos sean eficaces, eficientes, efectivos y transparentes. Todo esto lo hace posible la revisión y la acción constante de los indicadores, sin una efectiva medición del rendimiento, los otros cuatro aspectos del Gobierno TI es muy probable que fallen.

Una vez implementado el sistema de Gobierno de TI, este no debe permanecer inflexible ante los cambios en su entorno, sino que debe caracterizarse por su anticipación para afrontar cambios inesperados y planificar los esperados, tener agilidad en tiempos de respuesta, y adaptarse para auto aprender y auto organizarse con base en las experiencias anteriores.

5.3. GOBIERNO Y GESTIÓN DE IDENTIDADES DIGITALES Y DE ACCESOS

5.3.1. Identidad digital, roles y accesos

Una identidad electrónica es un conjunto de datos sobre una persona o entidad que determina en qué momento y a qué sistemas o lugares puede ésta acceder en una organización[7].

Entre los datos que conforman una identidad electrónica se tiene:

- Un identificador único (comúnmente llamado nombre de cuenta o usuario).
- La descripción de la persona o entidad a la cual se ha asignado el identificador (usualmente su nombre).
- Información de contacto de esa persona o entidad (correo electrónico, número telefónico, dirección de residencia/trabajo).
- Información organizacional de esa persona (id de su jefe o coordinador, departamento al que pertenece, su ubicación).
- Contraseña y/u otros factores de autenticación (huella, imagen del iris, tarjetas electrónicas).
- Permisos y restricciones (roles, grupos, accesos, horarios de acceso)

En general, un rol representa un conjunto de responsabilidades necesarias para llevar a cabo una transacción u operación del negocio, acceso representa los privilegios y recursos utilizados por alguien dentro de un rol. Una identidad representa a alguien o algo con un determinado rol en cierto momento del tiempo[8].

5.3.2. Gobierno y Gestión de identidades

El Gobierno de Identidades Digitales y Accesos consiste en como una organización define roles e identidades con la participación de los líderes del negocio responsables de las operaciones y transacciones que dependen de esos para roles para funcionar[8].

Por otra parte, la Gestión de Identidades Digitales y Accesos es la combinación de procesos de negocio, políticas de seguridad y tecnologías que apoyan a una organización en la administración del ciclo de vida de las identidades digitales y de control del acceso[9].

El ciclo de vida de una identidad incluye:

[7] Bertino, E., Takahashi, K.. (2010). Identity Management: Concepts, Technologies, and Systems.
[8] Etges, Rafael. (2011). The Impact of Governance on Identity Management Programs. ISACA.
[9] SANS. (2005). Identity and Access Management Solution.

- Activación: Todos los pasos que se llevan a cabo cuando, un nuevo empleado es contratado, un estudiante es matriculado, o un cliente o asociado se le permite acceder a un sistema.
- Administración: Los usuarios en general son dinámicos y esta fase incluye tareas tales como cambios de nombres, direcciones, permisos, responsabilidades, etc. Los cambios que experimentan los usuarios en el mundo real deben reflejarse en las definiciones de éstos en los sistemas y aplicaciones.
- Soporte: Los usuarios experimentan problemas con los sistemas y aplicaciones. Los cambios de contraseñas y en general todas las tareas para ayudar al usuario con su identificación electrónica están incluidas en esta fase.
- Desactivación: Cuando un usuario es retirado de una organización, todos los accesos a los diferentes sistemas o lugares deben ser retirados.

La siguiente figura resume los elementos que hacen parte del Gobierno y Gestión de Identidades Digitales y de Accesos.

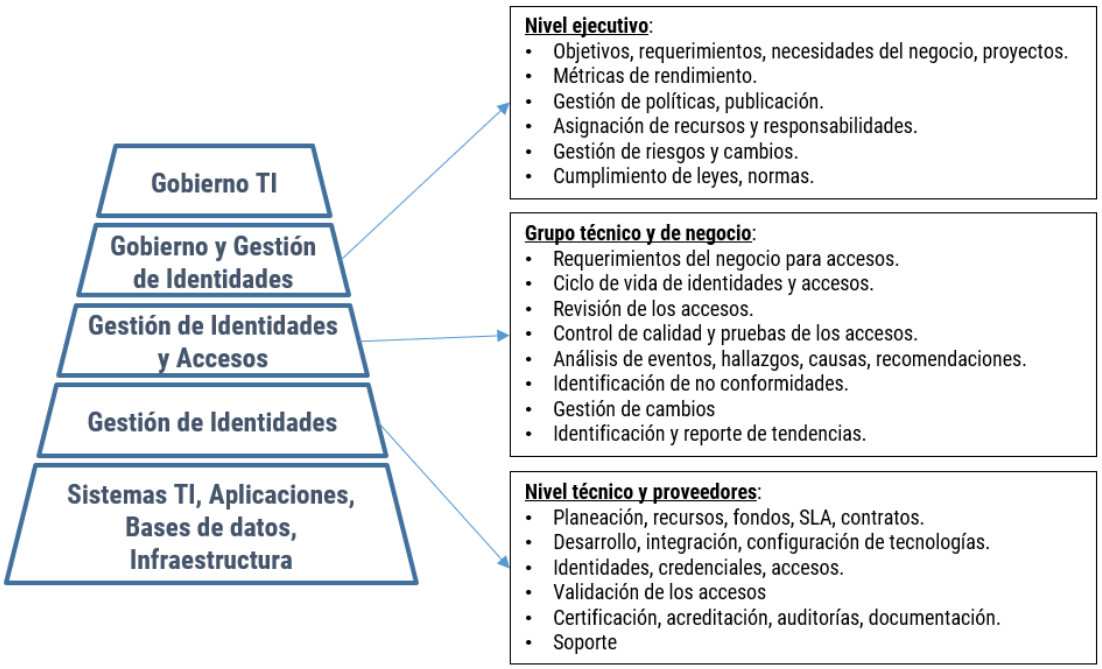

Figura 2. Gobierno y Gestión de Identidades. Adaptado de Etges[8]

5.3.3. Sistemas de Gestión de identidades

Un sistema de *gestión de identidades* es la infraestructura técnica que permite que una organización parametrice sus políticas, reglas de negocios, roles y permisos con el fin de automatizar el ciclo de vida de las identidades electrónicas.

Entre los beneficios que esto trae tenemos:

- Una gestión más rápida. Los usuarios no tienen que esperar por los cambios.
- Una gestión más eficiente. Se reducen los costos de administrar sistemas y aplicaciones.
- Una gestión más segura. Se reduce el riesgo de tener activas identificaciones de usuarios retirados o identificaciones con permisos no adecuados.

5.3.3.1 Componentes de un sistema de gestión de identidades

En general un sistema de gestión de identidades puede incluir uno o más procesos tales como:

- Auto activación. Por ejemplo se monitorea la aplicación de Recursos Humanos y automáticamente se crean nuevos usuarios en otros sistemas cuando un registro de un nuevo empleado es creado en la base de datos de RH.
- Auto desactivación. Por ejemplo, un empleado marcado como inactivo en la base de datos de RH, es automáticamente inactivado en otras aplicaciones.
- Sincronización de identidades. Si el nombre del usuario es modificado, automáticamente se actualiza en los otros sistemas.
- Autoservicio. Por ejemplo, un usuario modifica sus datos de contacto o solicita el reinicio de su contraseña.
- Solicitudes de acceso delegadas. Por ejemplo, un coordinador solicita el acceso a un sistema en nombre de sus subordinados.
- Flujos de autorizaciones. Por ejemplo, el aplicativo solicita a un gerente el aprobar o no una solicitud de cambio de permisos para un usuario.
- Certificaciones de acceso. Por ejemplo, periódicamente se le solicita a un coordinador que verifique si una lista de subordinados está vigente o no.

Usualmente un sistema de gestión de identidades incluye los siguientes componentes:

- Fuentes autoritativas: Sistema o sistemas en que los que se inicia el ciclo de vida de una identidad. Usualmente los sistemas donde se registran los datos básicos de una persona (ERP, software de gestión humana, registro de matriculas de estudiantes, etc.) hacen las veces de fuentes autoritativas. Estos sistemas se encargan de informar las novedades (existe un nuevo funcionario o estudiante, por ejemplo) para a partir de ello, inicializar todo el proceso de GdI.

- Conectores: se encargan de leer información de los usuarios en los sistemas integrados y enviar actualizaciones (activaciones, desactivaciones, etc.) a estos mismos sistemas.
- Base de datos interna: almacena la información de los usuarios, sistemas, políticas, permisos, etc.
- Directorios: aplicativos que ordenan la información de las identidades y permite realizar búsquedas y consultas de forma rápida. En estos un aplicativo puede buscar un usuario, validar su contraseña y determinar que accesos tiene dicho usuario. Usualmente se implementan siguiendo el protocolo LDAP.
- Sistemas de logon único: Protocolos o aplicativos que permiten luego de iniciar sesión (logon) en un único punto, acceder a varios programas sin necesidad de reescribir las credenciales. CAS, SAML y Open ID, entre otros, son ejemplos de ello.
- Sistemas de autoexploración: alimentan la base de datos utilizando los conectores.
- Interfaz de usuario: en ésta los usuarios pueden revisar el contenido de la base de datos, solicitar cambios, aprobar o denegar cambios, etc.
- Motor de flujo de autorizaciones. Permite implementar reglas y políticas para autorizar la generación de identidades, permisos, etc.
- Informes. Permite extraer información para controles, seguimientos y auditorías.

La siguiente figura muestra de manera general la forma más común de integrar un sistema de gestión de identidades. En este se muestra como el sistema de GdI toma los datos de un ERP, que hace las veces de fuente autoritativa, luego de ello asigna un id, roles y permisos al nuevo usuario para finalmente generar la identificación en el sistema o sistemas. Para el caso de las personas que se retiran, se les revocarán lo previamente concedido.

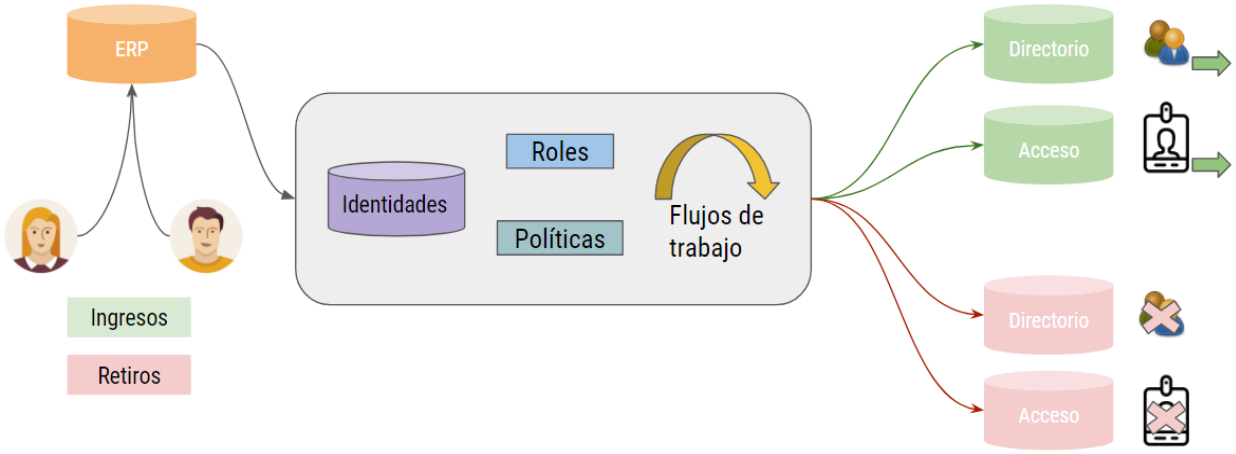

Figura 3. Diagrama general de un gestor de identidades

5.4. MARCOS Y CONJUNTO DE BUENAS PRÁCTICAS DE GOBIERNO DE REFERENCIA

5.4.1. COBIT 5

Un buen gobierno y una buena gestión de los activos de TI y de la información son requeridos para generar valor para las partes interesadas de una institución.

COBIT5 (Control Objectives for Information and related Technology) proporciona un marco integral que ayuda a las Organizaciones a lograr sus metas y entregar valor mediante un gobierno y una administración efectivos de la TI.

COBIT 5 es mantenido por ISACA (Information Systems Audit and Control Association) y el ITGI (IT Governance Institute).

COBIT 5 reúne una serie de mejores prácticas dirigida al control y supervisión de la Información, las Tecnologías de la Información y los riesgos relacionados, su orientación ayuda a las organizaciones a implementar efectiva gobernabilidad durante toda la empresa de TI[10] .

COBIT 5 se basa en cinco principios fundamentales para el Gobierno y la Gestión de TI:

1. Satisfacer las Necesidades de las Partes Interesadas.
2. Cubrir la Empresa de Extremo-a-Extremo.
3. Aplicar un solo marco integrado.
4. Habilitar un enfoque Holístico.
5. Separar el Gobierno de la Administración.

La figura 2 muestra los 37 procesos de gobierno y gestión de COBIT 5:

[10] ISACA. (2012). COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.

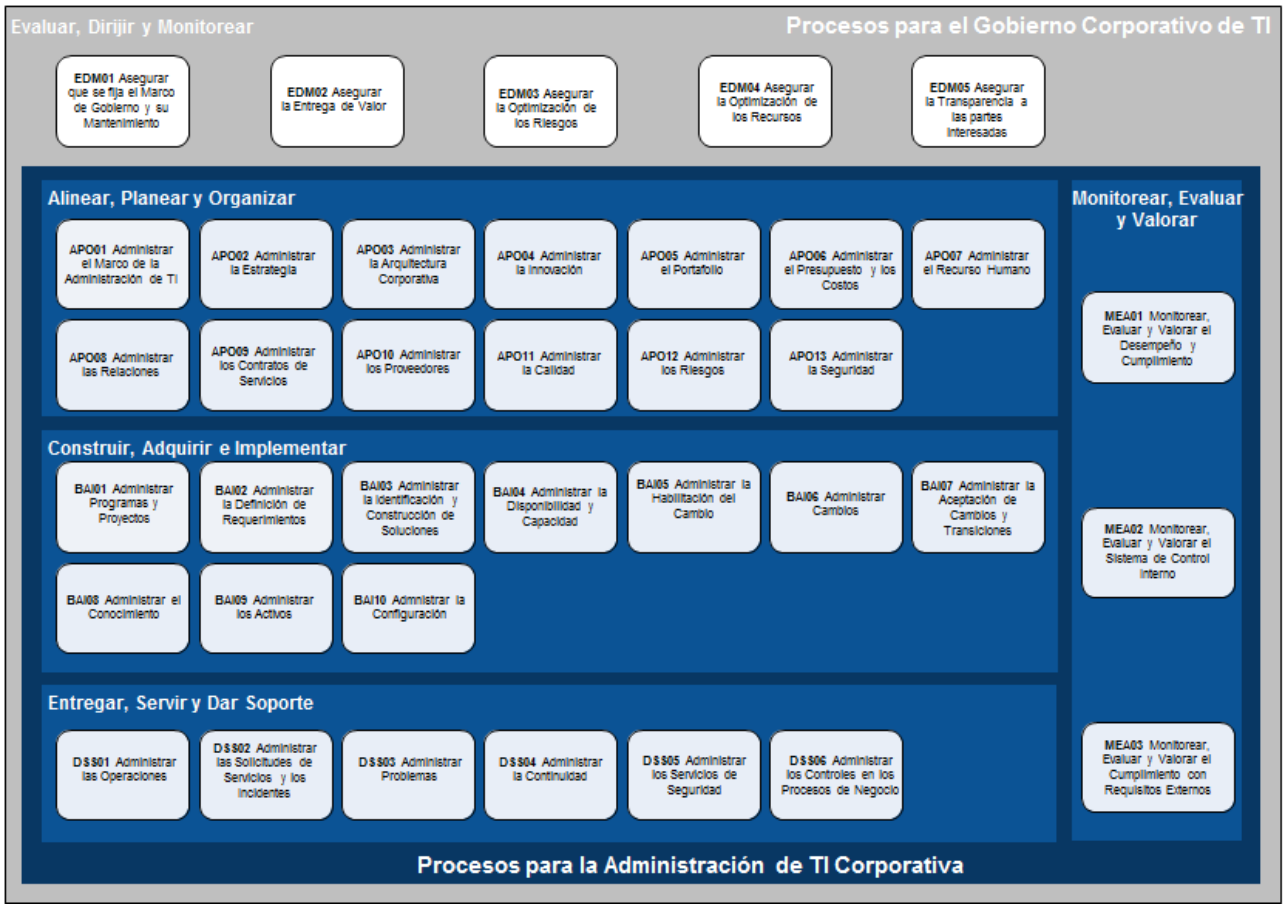

Figura 2: Conjunto Completo de los 37 procesos de gobierno y gestión dentro de COBIT 5.[11]

En lo que concierne a Gobierno y Gestión de Identidades digitales y de accesos, COBIT dos procesos directamente asociados como son Gestionar Servicios de Seguridad (DSS05) y Gestionar Controles de Proceso de Negocio (DSS06).

5.4.2. ISO 27001 e ISO 27002

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

[11] ISACA. (2012). COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.

ISO 27001 proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace determinando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo). La filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Por su parte ISO 27002 es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

ISO 27002 no es certificable. Contiene 35 objetivos de control y 144 controles, agrupados en 14 dominios. La norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2013.

Se debe tener presente que todos los controles no es posible aplicarlos. Además, se pueden requerir controles y directrices adicionales que no están incluidos en esta guía.

En lo que concierne a Gobierno y Gestión de Identidades digitales y de accesos, ISO 27002 incluye en el control 9 una serie de buenas prácticas para la implementación de una política de accesos.

5.4.3. ITIL 3

Es un conjunto de conceptos y mejores prácticas referentes a la gestión de servicios de tecnologías de la información (TI) con el fin de alinearlas con la estrategia de una compañía. ITIL describe detalladamente un extenso conjunto de funciones y procesos ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.

ITIL en su última versión, la 3, lanzada en 2007 y que fue actualizada en 2011, se estructura en los siguientes 5 libros con el objetivo de consolidar el modelo de “Ciclo de Vida del Servicio”:

1. Estrategia del Servicio.
2. Diseño del Servicio.

3. Transición del Servicio.
4. Operación del Servicio.
5. Mejora Continua del Servicio.

5.4.3.1. Estrategia del Servicio

En el centro del Ciclo de Vida del Servicio está la Estrategia del Servicio. Ésta promueve la visión de la gestión del servicio como un activo estratégico, y no sólo como una capacidad de la organización.

Los procesos asociados a la estrategia del servicio son los siguientes:

- Gestión financiera
- Gestión del portfolio de servicios
- Gestión de la demanda

5.4.3.2. Diseño del Servicio

En este libro, ITIL proporciona los principios de diseño y los métodos necesarios para convertir los objetivos de negocio estratégicos en un catálogo de servicios con sus activos asociados.

El principal objetivo del Diseño del Servicio es diseñar los servicios nuevos o modificados, de forma alineada con los objetivos de negocio establecidos en la Estrategia del Servicio, para incorporarlos al Catálogo de Servicios e implantarlos posteriormente en producción.

Los procesos asociados a la Estrategia del Servicio son los siguientes:

- Gestión del Catálogo de Servicios
- Gestión de Niveles de Servicio
- Gestión de la Capacidad
- Gestión de la Disponibilidad
- Gestión de la Continuidad
- Gestión de Proveedores
- Gestión de la Seguridad de la Información

5.4.3.3. Transición del Servicio

El principal objetivo de la etapa de Transición del Servicio es la implantación de los Servicios nuevos o modificados con el mínimo impacto para el negocio y dentro de los parámetros previstos de coste, tiempo y calidad.

Los procesos asociados a la Transición del Servicio son los siguientes:

- Planificación y soporte a la Transición
- Gestión de Cambios
- Gestión de la Configuración y Activos del Servicio
- Gestión de Versiones y Despliegues
- Validación y pruebas del Servicio
- Evaluación
- Gestión del Conocimiento

5.4.3.4. Operación del Servicio

La Operación del Servicio es la fase en la que realmente los servicios aportan valor al negocio y donde los planes, diseños y mejoras del Ciclo de Vida del Servicio son ejecutados y evaluados.

Los procesos asociados a la Operación del Servicio son los siguientes:

- Gestión de Eventos
- Gestión de Incidencias
- Gestión de Peticiones de Servicio
- Gestión de Problemas
- Gestión de Accesos

Las funciones asociadas a la Operación del Servicio son las siguientes:

- Service Desk
- Gestión de Operaciones TI
- Gestión Técnica
- Gestión de Aplicaciones

5.4.3.5. Mejora Continua del Servicio

El principal objetivo de la Mejora Continua del Servicio es alinear y realinear los servicios con las necesidades cambiantes de negocio identificando e implementando mejoras.

Los procesos asociados a la Mejora Continua del Servicio son los siguientes:

- Proceso de Mejora.
- Informes de Servicio.

5.5 CICLO DE DEMING

W. Edwards Deming en la década de 1950 propuso que los procesos de las compañías deberían analizarse y medirse para identificar las fuentes de variaciones que hacían que los productos se desviaran de los requisitos del cliente. Por ello recomendó que estos procesos de negocios mantuvieran un ciclo de retroalimentación continuo para que los gerentes pudieran identificar y cambiar las partes del proceso que necesitaran mejoras. Deming creó un diagrama para ilustrar este proceso continuo, comúnmente conocido como el ciclo PHVA[12]:

- Plan: Diseñar o revisar los componentes del proceso empresarial para mejorar los resultados.
- Hacer: Implementar el plan y medir su desempeño.
- Verificar: Evalúa las mediciones e informa los resultados a los tomadores de decisiones.
- Actuar: Decide los cambios necesarios para mejorar el proceso

[12] Arveson, Paul. (1998) The Deming Cycle. BSC. Recuperado de: http://www.balancedscorecard.org/BSC-Basics/Articles-Videos/The-Deming-Cycle.

6. MARCO DE REFERENCIA

6.1 USO DE GESTIÓN DE IDENTIDADES y ACCESOS EN UNIVERSIDADES

EDUCAUSE es una asociación sin fines de lucro cuya misión es promover la educación superior a través del uso de la tecnología de la información[13].

En el verano de 2016, 3.500 instituciones fueron invitadas a contribuir con datos al Servicio de Datos Básicos de EDUCAUSE (CDS). De este estudio EDUCAUSE publicó en 2017 "The EDUCAUSE Information Security Almanac"[14], en el cual resume los datos de las 607 instituciones que respondieron al módulo de seguridad de información opcional. Algunos datos públicamente disponibles del Sistema Integrado de Datos de Educación Postsecundaria (IPEDS, nces.ed.gov/ipeds/) se utilizaron para calcular las métricas. Las estadísticas informadas son una proporción estimada de la población o una mediana estimada (en lugar de una media).

A continuación, se muestran la información que se relaciona con Gestión de Identidades y Accesos:

- 64% de las universidades requieren autenticación en sus redes cableadas y 92% lo hacen en las inalámbricas. A su vez, el 57% le solicita autenticación a los invitados en la WLAN
- 1% usan biometría

Uso de autenticación multifactor:

- Aplicaciones críticas (finanzas, GH) (32%)
- Correo (10%)
- Acceso administrativo IT (8%)
- Acceso remoto (8%)

[13] https://www.educause.edu/about/mission-and-organization

[14] https://library.educause.edu/resources/2017/5/the-educause-information-security-almanac-2017

Otros datos importantes:

- Para el 69% de los encuestados, su principal preocupación es la seguridad de la información.
- En el 86% IT se encarga de la GIA.
- 3% del presupuesto de IT se destina a Seguridad Informática.
- 22% han implementado ISO 27001

Finalmente tenemos que en una encuesta realizada por EDUCAUSE en 2014 (Top Ten IT Issues 2014, Be the change you see) el 47% de los encuestados manifestó haber implementado alguna norma o marco (COBIT, ISO, NIST)

6.2 MERCADO DE SOFTWARE DE GESTIÓN DE IDENTIDADES Y ACCESOS

Gartner Inc. es una empresa con sede principal en USA cuyas actividades principales son la consultoría y la investigación sobre TI[15].

Gartner Inc. es muy conocida por analizar las tendencias del mercado y elaborar un ranking de publicación anual sobre soluciones tecnológicas, los cuales se conocen como los "cuadrantes de Gartner".

El Cuadrante Mágico de Gartner es una representación gráfica de la situación del mercado de un producto tecnológico en un momento determinado y se utiliza para tener una referencia del comportamiento del mercado mediante la posición relativa de productos y/o soluciones en el espacio del análisis de negocios[16].

En Junio de 2017 Gartner publicó un informe llamado "Magic Quadrant for Access Management, Worldwide" en el que además de resaltar los vendedores de software GIA visionarios y líderes del mercado, hacía estas anotaciones:

- La gestión de acceso (AM) se aplica a las tecnologías que utilizan motores de control de acceso para proporcionar autenticación centralizada, inicio de sesión único (SSO), gestión de sesiones y cumplimiento de autorización para aplicaciones de destino en casos de uso múltiple.
- Este Cuadrante Mágico se enfoca en proveedores que ofrecen funcionalidad AM para admitir múltiples casos de uso común, y que brindan soluciones en forma de dispositivos de hardware o software, o como un servicio para cumplir con los requisitos del cliente para el control de acceso a aplicaciones y servicios locales o privados y nubes públicas.

[15] www.gartner.com

[16] http://www.bigdata-social.com/informe-cuadrante-magico-gartner/

Además se permitieron hacer estas proyecciones en dicho mercado:

- Para el año 2019, más del 80% de las organizaciones utilizará software o servicios de administración de acceso, en comparación con el 55% actual.
- Para el año 2021, IDaaS será el modelo de administración de acceso mayoritario para nuevas compras, en comparación con menos del 20% actual.

Figura 4. Magic Quadrant for Access Management, Worldwide. Gartner. 2017.

6.3 TENDENCIAS

Entre las tendencias más importantes en GGIA tenemos[17]:

- Aumento del uso de:
  - Inicio de sesión único (SSO).
  - Autenticación de factor múltiple.
  - Autenticación sin contraseña.
  - GIA como servicio (cloud).
  - Mobile ID: uso de dispositivos móviles con diferentes elementos (fotos, hologramas, códigos QR, etc) para facilitar la identificación con el fin de reemplazar las clásicas tarjetas de PVC impresas (carnés).
  - Fast IDentity Online (FIDO) - IA para acelerar los procesos de identificación y aumentar su confiabilidad.

- Uso de analítica de datos del comportamiento de los usuarios: GIA sabe quiénes somos, cuando estamos activos y nuestros hábitos de navegación. Se espera que en los próximos años el uso de esta información en mercadeo y en la prevención de amenazas aumente.

- Uso de blockchain para descentralizar la infraestructura GIA.

- GIA para robots industriales, IoT

[17] https://silasg.com/insights/2018-trends-predictions-identity-management
https://securityintelligence.com/current-trends-in-identity-and-access-management-july-2017/
https://www.onelogin.com/blog/top-3-iam-trends-to-watch-for-in-2018
https://www.gartner.com/smarterwithgartner/identity-and-access-management-in-the-digital-age/

7. PROTOCOLO DE GOBIERNO Y GESTIÓN DE IDENTIDADES DIGITALES Y ACCESO

7.1. PROTOCOLO PROPUESTO

La siguiente figura muestra el protocolo de Gobierno y Gestión de Identidades digitales y acceso que se propone:

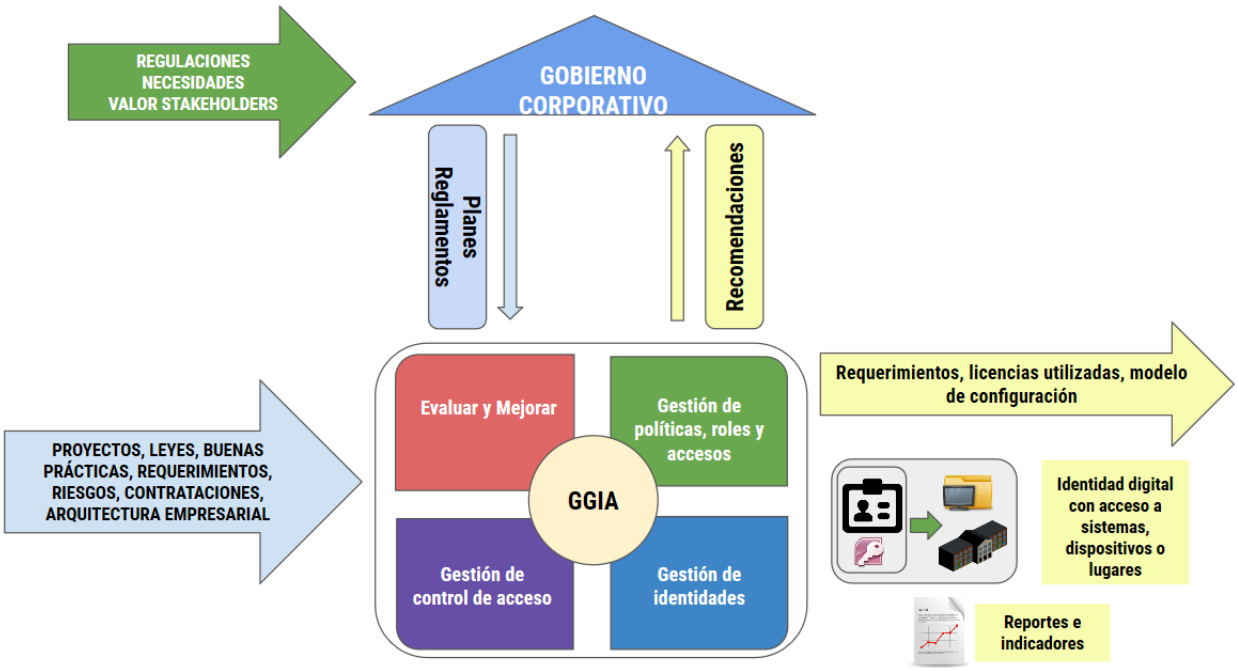

Figura 5. Protocolo de Gobierno y Gestión de Identidades digitales y acceso
Fuente: propia

Entre las principales características del protocolo planteado tenemos:

- Incluye los componentes del Gobierno Corporativo y su interacción con el Gobierno IT y la Gestión de Identidades Digitales y de Acceso. El Gobierno

corporativo emite planes y reglamentos que son recibido por el protocolo para alinearse al negocio.

- El gobierno se encargará de Evaluar, Supervisar y Monitorear la gestión.
- La gestión describe los procesos, procedimientos y proyectos para la operación de la institución en el contexto de las identidades digitales y el acceso.
- Basado en COBIT 5, ISO 27002 e ITIL 3.
- Implementa el ciclo de Deming con las actividades Gestión de políticas, roles y accesos (planear), Gestión de identidades (hacer), Gestión de control de acceso (verificar) y evaluar y mejorar (actuar). Esto facilita implementarlo en organizaciones que ya tengan implementados procesos siguiendo los lineamientos de normas como ISO 9001, ISO 27001, marcos como COBIT o buenas prácticas como ITIL, entre otros.
- Como entradas se consideran salidas de otros procesos y actividades como: proyectos, contratos, leyes, reglamentos, normativas, buenas prácticas, requerimientos (solicitudes, cambios, incidentes), riesgos y lineamientos de la Arquitectura Empresarial.
- En las salidas del protocolo tenemos: identidades digitales con acceso a sistemas, dispositivos o lugares, requerimientos (solicitudes, cambios, incidentes), licencias utilizadas, Modelos de configuración, reportes e indicadores.

GOBIERNO Y GESTIÓN DE IDENTIDADES Y ACCESOS							
Gestión de políticas, roles y accesos		Gestión de identidades		Gestión de control de acceso		Evaluar y mejorar	
Referencia	**Subproceso**	**Referencia**	**Subproceso**	**Referencia**	**Subproceso**	**Referencia**	**Subproceso**
COBIT APO01	Gestionar el Marco de Gestión de TI	COBIT BAI02	Gestionar la definición de requisitos GIA	COBIT DSS05	Gestionar servicios de seguridad	COBIT MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad GIA
COBIT APO02	Gestionar la Estrategia GIA	COBIT BAI06	Gestionar los Cambios GIA	COBIT DSS06	Gestionar controles de procesos corporativos	COBIT MEA03	Supervisar, Evaluar y Valorar la Conformidad GIA con los Requerimientos Externos
27002 Control 9	Gestionar la Política de control de acceso	COBIT BAI09	Gestionar los activos GIA	ITIL	Gestión de Acceso		
		COBIT BAI10	Gestionar la configuración GIA				

Tabla 2. Subprocesos del protocolo planteado (basado en COBIT 5, ISO 27002 e ITIL 3)
Fuente propia

7.2 ACTIVIDADES Y LINEAMIENTOS DEL PROTOCOLO

7.2.1 Gestión de políticas, roles y accesos

7.2.1.1 Gestionar el Marco de Gestión de TI

Objetivo: definir la propiedad de la información (datos) y del sistema (COBIT APO01.06)

Actividades:

1. Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información (datos) asociada a la GIA.
2. Definir, mantener y proporcionar herramientas adecuadas, técnicas y directrices para garantizar la seguridad y control efectivo sobre la información y los sistemas en colaboración con el propietario.
3. Crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones. Incluir los sistemas subcontratados y aquellos cuya propiedad debe permanecer dentro de la empresa.
4. Definir e implementar procedimientos para asegurar la integridad y consistencia de toda la información almacenada en formato electrónico, tales como bases de datos, almacenes de datos (data warehouses) y archivos de datos.

7.2.1.2. Gestionar la Estrategia GIA

Objetivo: entender la dirección corporativa (COBIT APO02.01)

Actividades:

1. Desarrollar y mantener un entendimiento de las estrategias y objetivos del negocio, así como del entorno y los retos operativos actuales.
2. Desarrollar y mantener un entendimiento del entorno externo a la empresa.
3. Identificar las partes interesadas más importantes y obtener comprensión de sus requerimientos.
4. Identificar y analizar las fuentes de los cambios en la empresa y en el entorno externo.
5. Determinar prioridades para el cambio estratégico.
6. Entender la actual arquitectura de empresa y trabajar con el proceso de arquitectura de la empresa para determinar cualquier brecha potencial en la arquitectura

7.2.1.3. Gestionar la política de control de acceso

Objetivo: Establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información (ISO 27002, Control 9)

Lineamientos:

1. Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
2. Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
3. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
4. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
5. La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
6. Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
7. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
8. Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.

Otros lineamientos puntuales para Instituciones de Educación Superior:

1. Definir una fuente, usualmente llamada autoritativa, en lo posible única, que provea la información de las identidades que se almacenarán en el repositorio de la organización. Si bien en otras industrias el software de recursos humanos es la fuente usual, para el caso de las IES no siempre se cuenta con un ERP que contenga tanto la información de empleados como la de estudiantes. Si bien se pueden tener varias fuentes, se debe definir cuál es autoritativa para cada caso.
2. Se recomienda consolidar las identidades en un repositorio centralizado.
3. Establecer los roles de negocio que soportan la operación y alinearlos a los roles a implementar en los diferentes servicios TIC.
4. Definir los procedimientos de asignación de roles teniendo como premisa la de otorgar siempre el menor privilegio necesario.
5. Establecer un procedimiento de asignación de una identificación única, irrepetible y no reusable para cada entidad.
6. Definir en lo posible varios factores de autenticación según la criticidad de la aplicación o por el nivel de riesgo de la misma.
7. Definir de ser el caso identidades federadas de tal forma que la misma identidad se pueda acceder a servicios de entidades o redes diferentes.

8. Cifrado de contraseñas. Estas deben intercambiarse y guardarse de forma segura.
9. Establecer un perfil básico de servicios y permisos a otorgar a todos los miembros para cada uno de los grandes grupos de una IES como son entre otros: profesores, estudiantes, empleados, egresados, contratistas, pensionados.

7.2.2. Gestión de identidades

7.2.2.1. Gestionar la definición de requisitos GIA

Objetivo: Definir y mantener los requerimientos técnicos y funcionales de negocio (COBIT BAI02.01)

Actividades:

1. Definir e implementar la definición de requerimientos y el procedimiento de mantenimiento y un repositorio de requisitos acorde al tamaño, complejidad, objetivos y riesgos de la iniciativa que la empresa está considerando acometer.
2. Expresar los requerimientos de la empresa en términos de cómo la diferencia entre las capacidades de negocio existentes y deseadas son tratadas y como cada rol interactuará con la solución y la utilizará.
3. Durante todo el proyecto, obtener, analizar y confirmar que los requerimientos de todas las partes interesadas, incluyendo los criterios de aceptación relevantes, son considerados, obtenidos, priorizados y registrados de un modo comprensible para las partes interesadas, patrocinadores de negocio y personal de la implementación técnica, reconociendo que los requerimientos pueden cambiar y llegar a ser más detallados según se implementen.
4. Especificar y priorizar la información, los requerimientos técnicos y funcionales basados en los requerimientos de las partes interesadas. Incluir requerimientos de control de la información en los procesos de negocio, procesos automatizados y entornos de TI para hacer frente a los riesgos de la información y cumplimiento con regulaciones, leyes y contratos comerciales.
5. Validar todos los requerimientos mediante aproximaciones tales como revisión por iguales, validación del modelo o prototipo operativo.
6. Confirmar la aceptación de aspectos clave de los requerimientos, incluyendo reglas de negocio, controles de información, continuidad de negocio, cumplimiento legal y regulatorio, ‘auditabilidad’, ergonomía, operatividad y usabilidad, seguridad y soporte documental.
7. Hacer seguimiento y controlar el alcance, los requerimientos y los cambios a lo largo del ciclo de vida de la solución durante el proyecto según evolucione la comprensión de la solución.
8. Considerar los requerimientos relativos a políticas y estándares empresariales, arquitectura empresarial, planes TI estratégicos y tácticos, procesos de TI internos y externalizados, requerimientos de seguridad, requerimientos

regulatorios, competencias del personal, estructura organizativa, caso de negocio y tecnologías catalizadoras.

7.2.2.2. Gestionar los cambios GIA

Objetivo: Evaluar, priorizar y autorizar peticiones de cambio (COBIT BAI06.01)

Actividades:

1. Utilizar peticiones de cambio formales para posibilitar que los propietarios de procesos de negocio y TI soliciten cambios en procesos de negocio, infraestructura, sistemas o aplicaciones. Asegurar que todos estos cambios surgen sólo a través del proceso de gestión de las peticiones de cambio.
2. Categorizar todas las peticiones de cambio (ej. procesos de negocio, infraestructura, sistemas operativos, redes, sistemas de aplicación, software externo adquirido) y relacionarlas con los elementos de configuración afectados.
3. Priorizar todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio, recursos necesarios, así como las razones contractuales, legales o de regulación que motivan el cambio.
4. Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio (BCPs) y proveedores de servicios para asegurar que todos los componentes afectados han sido debidamente identificados. Evaluar la probabilidad de que afecten negativamente el entorno operativo y el riesgo de implementar el cambio. Considerar las implicaciones de seguridad, legales, contractuales, y de cumplimiento normativo del cambio solicitado. Considerar además todas las interdependencias entre cambios. Involucrar a los propietarios de procesos de negocio en el proceso de evaluación, de forma apropiada.
5. Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser pre-aprobados como cambios estándar.
6. Planificar y programar todos los cambios aprobados.
7. Considerar el impacto en los proveedores de servicios contratados (ej. procesamiento de negocio externalizado, infraestructuras, desarrollo de aplicaciones y servicios compartidos) en el proceso de gestión del cambio, incluyendo la integración de la gestión de cambios organizativos con los procesos de gestión de cambios de los proveedores de servicios y el impacto en términos contractuales y ANSs.

7.2.2.3. Gestionar los activos GIA

Objetivo: Administrar licencias GIA (BAI09.05)

Actividad:

1. Comparar el número de copias de software instalado con el número de licencias en propiedad.

7.2.2.4. Gestionar la configuración GIA

Objetivo: Establecer y mantener un modelo de configuración GIA (COBIT BAI10.01)

Actividad:

1. Definir y acordar el alcance y nivel de detalle para la gestión de la configuración (p.ej., qué servicios, activos y elementos configurables de la infraestructura se incluyen).
2. Establecer y mantener un modelo lógico para la gestión de la configuración, incluyendo información sobre los tipos de elementos de configuración, atributos de los elementos de configuración, tipos de relaciones, atributos de relación y códigos de estado.

7.2.3. Gestión de control de acceso

7.2.3.1. Gestionar servicios de seguridad GIA

Objetivo: Gestionar la seguridad de la red y las conexiones, la identidad del usuario y el acceso lógico (COBIT DSS05.02 y COBIT DSS05.04)

Actividades:

1. Permitir sólo a las personas y dispositivos autorizados tener acceso a la información y a la red de la empresa. En cualquier caso debería forzarse a solicitar una contraseña.
2. Cifrar la información en tránsito de acuerdo con su clasificación.
3. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.
4. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.

5. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.
6. Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.
7. Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.
8. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.
9. Segregar y gestionar cuentas de usuario privilegiadas.
10. Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.
11. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.
12. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.

7.2.3.2. Gestionar controles de procesos corporativos

Objetivo: Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización y asegurar los activos de información (COBIT DSS06.03 y DSS06.06)

Actividades:

1. Asignar roles y responsabilidades sobre la base de la descripción aprobada de puestos y actividades de procesos de negocio asignadas.
2. Asignar niveles de autoridad para la aprobación de transacciones, límites y cualquier otra decisión relativa a los procesos de negocio, basadas en los roles de trabajo aprobados.
3. Asignar derechos de acceso y privilegios sólo sobre lo que es necesario para ejecutar las actividades de trabajo, basados en los roles de puesto predefinidos. Eliminar o revisar los derechos de acceso inmediatamente si el rol del puesto cambia o un miembro del personal deja el área de proceso de negocio. Revisar

periódicamente para asegurar que el acceso es adecuado para las actuales amenazas, riesgos, tecnología y necesidades del negocio.
4. Asignar roles para las actividades sensibles de manera que haya una segregación clara de funciones.
5. Proporcionar concienciación y formación en relación a los roles y responsabilidades de forma regular para que todo el mundo entienda sus responsabilidades; la importancia de los controles; y la integridad, confidencialidad y privacidad de la información de la empresa en todas sus formas.
6. Revisar periódicamente las definiciones de control de acceso, registros e informes.
7. Aplicar las políticas de clasificación de datos y uso aceptable y seguridad y los procedimientos para proteger los activos de información bajo el control del negocio.
8. Proporcionar concienciación y formación de un uso aceptable.
9. Restringir el uso, la distribución y el acceso físico a la información acorde a su clasificación.
10. Identificar e implementar procesos, herramientas y técnicas para verificar razonablemente el cumplimiento.
11. Informar al negocio y otros grupos de interés acerca de violaciones y desviaciones.

7.2.4. Evaluar y mejorar

7.2.4.1. Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad

Objetivo: Establecer un enfoque de la supervisión (COBIT MEA01.01)

Actividades:
1. Identificar las partes interesadas (p. ej. dirección, propietarios de procesos o usuarios).
2. Involucrar a las partes interesadas y comunicar los objetivos y requisitos empresariales para la supervisión, consolidación e información, utilizando definiciones comunes (p. ej. glosario corporativo, metadatos y taxonomías), líneas de referencia y estudios comparativos (benchmarking).
3. Mantener y alinear de forma continua el enfoque de supervisión y evaluación con el enfoque de la compañía, así como las herramientas utilizadas para la obtención de datos y presentación de informes corporativos.
4. Acordar los objetivos y métricas (p. ej., cumplimiento, rendimiento, valor, riesgo), taxonomía (clasificación y relación entre objetivos y métricas) y la retención de datos (evidencias).

5. Acordar un proceso de control de cambios y de gestión del ciclo de vida de la supervisión y la presentación de informes. Incluir oportunidades de mejora para la presentación de la información, métricas, enfoque, líneas de referencia y estudios comparativos.
6. Solicitar, priorizar y reservar recursos para la supervisión (considerando oportunidad, eficiencia, efectividad y confidencialidad).
7. Validar periódicamente el enfoque utilizado e identificar los nuevos o cambiantes grupos de interés, requisitos y recursos.

7.2.4.2. Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

Objetivo: Identificar requisitos externos de cumplimiento (COBIT MEA03.01)

Actividades:

1. Asignar la responsabilidad de identificar y supervisar los cambios legales y regulatorios y otros requisitos contractuales externos aplicables a la utilización de recursos de TI y al procesamiento de la información dentro de las operaciones de negocio y de TI.
2. Identificar y valorar la totalidad de los posibles requisitos de cumplimiento y su impacto sobre las actividades de TI en ámbitos como los flujos de datos, la privacidad, los controles internos, los informes financieros, la regulación sectorial, la propiedad intelectual y la seguridad e higiene en el trabajo.
3. Valorar el impacto de los requisitos legales y regulatorios relacionados con TI sobre los contratos con terceros que afecten a las operaciones de TI, los proveedores de servicio y los socios de negocio.
4. Obtener asesoramiento independiente, si procede, sobre las modificaciones en las legislaciones, regulaciones y estándares aplicables.
5. Mantener un inventario actualizado de los requisitos legales, regulatorios y contractuales aplicables, su impacto y las acciones necesarias.
6. Mantener un registro general consolidado de los requisitos externos de cumplimiento que afecten a la empresa.

7.3 ROLES

A continuación, se muestra la matriz de roles del proceso (RACI) la cual se basa en COBIT 5.

Referencia	Proceso	Actividad	Alta Gerencia	Director Financiero	Director Area responsable	Ejecutivos de Negocio	Propietario Proceso Negocio	Cómite Estrategico	Director Recursos Humanos	Cumplimiento Normativo	Auditoria	Director TI	Arquitecto TI	Jefe Seguridad	Jefe Desarrollo	Jefe Operaciones	Gestor Servicios TI	Gestor Seguridad	Gestor Privacidad
COBIT-APO01	Gestionar el Marco de Gestión de TI	APO01.06-Definir la propiedad de la información (datos) y del sistema	I	I	C	C	R		C	C	C	C	C						C
COBIT-APO02	Gestionar la Estrategia GIA	APO02.01-Entender la dirección corporativa	C	C	C	A	C					R	A				R	R	
COBIT-BAI02	Gestionar la definición de requisitos GIA	BAI02.01Definir y mantener los requerimientos técnicos y funcionales de negocio				I	R	A		C			R				C	C	C
COBIT-BAI06	Gestionar los Cambios GIA	BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio				A	R			C	C	R	I						
COBIT-BAI09	Gestionar los activos GIA	BAI09.05-Administrar licencias.				I	C			C	R	A			R	R	C		
COBIT-BAI10	Gestionar la configuración GIA	BAI10.01 Establecer y mantener un modelo de configuración.					C				C	C	C		I	A	R		
COBIT-DSS05	Gestionar servicios de seguridad GIA	DSS05.02-Gestionar la seguridad de la red y las conexiones.					I			C	C	C	I	A	R	R	I	R	
		DSS05.04-Gestionar la identidad del usuario y el acceso lógico.					R		I	C	C	C	I	A	C	R	I	R	C
COBIT-DSS06	Gestionar controles de procesos corporativos	DSS06.03-Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.		R	R	A	R		I	C	C	C		I		C	C	R	C
		DSS06.06-Asegurar los activos de información.		C	C	C	A			C	C	C		I		C		C	C
COBIT-MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	MEA01.01 Establecer un enfoque de la supervisión	A	R	R	R	I	C	C	C	C	R	I	C	C	C	C	I	I
COBIT-MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	MEA03.01 Identificar requisitos externos de cumplimiento				A	R			R	R	R							R

Tabla 3. Matriz RACI del protocolo GGIA (basado en COBIT 5)
Fuente propia

7.4 MÉTRICAS

La tabla 4 muestra las métricas que se establecieron para el protocolo GGIA. Estas se basan en COBIT 5.

Subproceso	Métrica
Gestionar el Marco de Gestión de TI	Número de problemas de no conformidad relativos a GIA de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos
	Número de incidentes relacionados con el incumplimiento de la política GIA
	Frecuencia de revisión y actualización de las políticas GIA
Gestionar la Estrategia GIA	Nivel de satisfacción de las partes interesadas con el alcance del portafolio GIA
	Número de interrupciones del negocio debido a incidentes en el servicio de GIA
	Porcentaje de usuarios satisfechos con la calidad de los servicios de GIA entregados
Gestionar la definición de requisitos GIA	Porcentaje de requerimientos repetidos debido a la no alineación entre las necesidades y expectativas de la organización
	Nivel de satisfacción de las partes interesadas con los requerimientos
Gestionar los Cambios GIA	Cantidad de trabajo rehecho debido a cambios fallidos
	Reducción en el tiempo y esfuerzo necesarios para aplicar los cambios
	Ratios de satisfacción de las partes interesadas con las comunicaciones de los cambios
Gestionar los activos GIA	Porcentaje de licencias usadas respecto a licencias pagadas
Gestionar la configuración GIA	Número de desviaciones entre el repositorio de configuración y la configuración real.
Gestionar servicios de seguridad GIA	Número de incidentes relacionados con accesos no autorizados a la información
Gestionar controles de procesos corporativos	Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados

	Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública
	Número de cuentas (con respecto al número de usuarios/empleados autorizados)
	Promedio de tiempo entre los cambios y actualizaciones de cuentas
	Número de incidentes relacionados con accesos no autorizados a la información
Gestión de Acceso	Número de solicitudes de acceso (Peticiones de servicios, solicitudes de cambio, etc.)
	Cantidad de accesos concedidos por servicio, usuario, departamento, etc.
	Número de incidentes que requirieron el reinicio de los derechos de acceso
	Número de incidentes causados por una incorrecta asignación de accesos
Supervisar, Evaluar y Valorar Rendimiento y Conformidad GIA	Porcentaje de informes de rendimiento entregados en plazo
	Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos
Supervisar, Evaluar y Valorar la Conformidad GIA con los Requerimientos Externos	Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI

Tabla 4. Métricas del protocolo GGIA (basado en COBIT 5)
Fuente propia

7.5 HERRAMIENTA DE MEDICIÓN DE NIVEL DE MADUREZ DEL PROTOCOLO

Para evaluar el nivel de madurez de una organización con respecto al protocolo GGIA propuesto se creó una herramienta que consiste en 35 preguntas cuyo objetivo es evaluar el nivel de implementación de las principales actividades de los diferentes subprocesos.

El cuestionario de las 35 preguntas se lista a continuación:

Proceso	Pregunta	
Gestionar Política de Control de acceso	1	¿Se cuenta con una política de control de acceso con base en los requisitos del negocio y de seguridad de la información?
	2	¿En caso de contar con una política, esta es revisada periódicamente?
	3	¿Dicha política contempla a los funcionarios, profesores, estudiantes, egresados, proveedores, contratistas y en general toda la comunidad que requiere acceso?
Gestionar el Marco de Gestión de TI	4	¿Se cuenta con un procedimiento para definir y mantener responsabilidades sobre la propiedad de la información (datos) y de los sistemas?
	5	¿Se cuenta con un procedimiento para crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones?
Gestionar la Estrategia GGIA	6	¿Se evalúa el rendimiento del negocio actual, las capacidades y los servicios TI externos y se comprende la arquitectura corporativa en relación con el GGIA?
	7	¿Se Identifican asuntos relevantes que hayan ocurrido y se desarrollan recomendaciones en áreas que puedan mejorar el GGIA?
Gestionar la definición de requisitos GGIA	8	¿A partir de la base del modelo conceptual de negocio, se identifica, prioriza, específica y acuerdan los requisitos funcionales, técnicos, de información y de control?
Gestionar los Cambios GGIA	9	¿Se evalúan todas las peticiones de cambio GGIA para determinar el impacto en el negocio y los procesos y servicios de IT, y para evaluar si el cambio afectará de forma negativa al entorno operacional o si introducirá algún riesgo no aceptable?
	10	¿Se Asegura que los cambios son registrados, priorizados, categorizados, analizados, autorizados y planificados?
Gestionar los activos GGIA	11	¿Al activar una identidad digital se tiene en cuenta que se cuente con licencias disponibles?

Gestionar la configuración GGIA	12	¿Se establece y mantiene un modelo lógico de los servicios, activos e infraestructura y sobre cómo registrar los ítems de configuración (CIs) y las relaciones entre ellos?
	13	¿Se incluyen los CIs considerados necesarios para gestionar eficazmente los servicios y proveer una descripción única y confiable de los activos de un servicio?
Gestionar servicios de seguridad GGIA	14	¿Todos los usuarios tienen un único identificador y los derechos de acceso acordes con su función en la empresa?
	15	¿Se asegura que todos los usuarios tienen derechos de acceso a la información acordes con sus requisitos de negocio?
	16	¿Se coordinar con las unidades par que gestionen sus propios derechos de acceso en los procesos de negocio?
	17	¿Se permite únicamente el acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente?
	18	¿Se cuenta con un proceso formal de registro y de cancelación de registro de usuarios que posibilita la asignación de los derechos de acceso?
	19	¿Se cuenta con un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios?
	20	¿Se restringe y controla la asignación y uso de cuentas de acceso privilegiado (administración, root)?
	21	¿Se cuenta con un proceso formal para la asignación secreta de contraseñas?
	22	¿Los propietarios de los activos revisan con una frecuencia determinada los derechos de acceso de los usuarios?
	23	¿Los derechos de acceso a aplicativos o lugares de profesores, funcionarios, estudiantes, egresados o proveedores son retirados al terminar su empleo, contrato o acuerdo, o se ajustan cuando se hacen cambios?
	24	¿Las contraseñas se cifran cuando son transmitidas o almacenadas?
	25	¿Se cuenta con una opción que permita los usuarios recordar su identificación de acceso a los servicios TI?
	26	¿Se cuenta con un metadirectorio de usuarios como LDAP o Active Directory con el fin de centralizar los usuarios?
	27	¿Se cuenta con herramientas de logon ùnico como CAS, SAML,

		OpenID, etc con el fin de facilitar el acceso a los usuarios?
	28	¿Se cuenta con una solución de gestión de identidades que facilita la automatización de las políticas establecidas?
	29	¿Se cuenta con una opción que permite a los usuarios reasignar de forma segura su contraseña en caso de olvido?
Gestionar controles de procesos corporativos	30	¿El inventario de funciones, responsabilidades y derechos de acceso está alineado con las necesidades de negocio autorizadas?
	31	¿Se administran las funciones de negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de proceso del negocio?
	32	¿Se gestiona la autorización al acceso a los recursos de información relacionados con los procesos de información, incluyendo los custodiados por la empresa, por TI y por terceros?
Supervisar, Evaluar y Valorar Rendimiento y Conformidad GIA	33	¿Se involucran a las partes interesadas y se comunican los objetivos y requisitos del proceso?
	34	¿Se tienen definidos objetivos, métricas y la retención de datos (evidencias)?
Supervisar, Evaluar y Valorar la Conformidad GIA con los Requerimientos Externos	35	¿Se identifican y valoran la totalidad de los posibles requisitos de cumplimiento y su impacto sobre las actividades de GGIA en ámbitos como los flujos de datos, la privacidad, los controles internos, los informes financieros, la regulación sectorial, la propiedad intelectual y la seguridad e higiene en el trabajo?

Tabla 5. Criterios de evaluación nivel de madurez.
Fuente: Adaptación propia de COBIT 5, ISO 27002 e ITIL 3.

Para la evaluación se adaptaron los criterios de evaluación de Selig como se muestra a continuación.

Nivel	Descripción	Observaciones
1	Proceso inicial (adhoc)	Proceso impredecible, mal controlado, reactivo
2	Proceso repetible	Los requisitos son gestionados y de que los procesos se planifican, realizan, medido y controlado.
3	Proceso Estandarizado e institucionalizado	Los procesos están bien caracterizados y entendidos, y se describen en las normas, procedimientos, herramientas y métodos
4	Proceso administrado	Los procesos están controlados mediante técnicas estadísticas y otras técnicas cuantitativas.
5	Proceso optimizado	Los procesos se basan en una comprensión cuantitativa de las causas comunes de variación inherentes a estos

Tabla 6. Criterios de evaluación nivel de madurez.
Fuente: Adaptación propia de Selig, G, Implementing IT Governance

El procedimiento para la evaluación es como sigue:

- Se responde cada pregunta de 1 a 5 conforme la actividad o tarea cumpla con el nivel especificado.
- Al final se toma un promedio para cada proceso.
- Se determinan cuáles fueron las respuestas más bajas.
- Se plantean planes o tareas que aumenten el respectivo nivel.
- Cumplido el plan o las tareas, se vuelve a evaluar para determinar el nivel de madurez alcanzado.

8. CASO DE ESTUDIO

8.1. FUNDACIÓN UNIVERSIDAD DEL NORTE

La Fundación Universidad del Norte es una institución de educación superior fundada en 1966 y ubicada en el área metropolitana de Barranquilla, Colombia. En el año 2003 recibió la A*creditación institucional de Alta Calidad* por parte del Ministerio de Educación por sus altos estándares académicos[18]. Esta acreditación le fue renovada por 8 años en 2010 y posteriormente en 2018 por el mismo período de tiempo. Junto a esto se tiene que sus procesos administrativos están certificados bajo la norma ISO 9001:2015.

8.1.1 Misión de la Universidad del Norte

La FUNDACIÓN UNIVERSIDAD DEL NORTE, acorde con los principios, valores y objetivos que la guían desde su creación, tiene como misión la formación integral de la persona en el plano de la educación superior, y la contribución, mediante su presencia institucional en la comunidad, al desarrollo armónico de la sociedad y del país, especialmente de la Región Caribe Colombiana.

La Fundación cumple esta labor universitaria tanto en la modalidad de pregrado como en la formación avanzada caracterizándose su quehacer por un amplio contenido social y humanístico, y por el énfasis en la fundamentación científica e investigativa para responder a los requerimientos del progreso de la ciencia y a las necesidades sociales de la región y del país.

Busca la Institución formar a sus estudiantes como personas pensantes, analíticas y de sólidos principios éticos, que conciban ideas innovadoras a fin de que participen de manera activa, emprendedora, responsable, honesta, crítica y pragmática en el proceso de desarrollo social, económico, político y cultural de la comunidad.

La Universidad propende por que la formación que en ella se imparte se realice con profesorado idóneo, calificado y con profunda vocación académica. Para apoyarlos en esa tarea, está decidida a contar con los métodos de enseñanza, de investigación y de extensión más adecuados y avanzados de la educación superior contemporánea. En este sentido, la ciencia, la tecnología, las humanidades y las artes seguirán siendo los ejes institucionales distintivos para la formación del estudiante.

[18] https://www.uninorte.edu.co/web/sobre-nosotros/nuestra-historia

Presente en la vida de la comunidad mediante el ejercicio de sus funciones académicas (docencia, investigación, extensión y servicios al sector externo), la Universidad del Norte procura que sus directivos, profesores, estudiantes y exalumnos se mantengan en permanente estudio, análisis e investigación de los problemas concretos de la comunidad en que se encuentran.

Nuestra institución está comprometida desde sus orígenes, en el presente y hacia el futuro, con todas las dimensiones del desarrollo social, económico, político, ambiental y cultural con responsabilidad social manteniéndose en su lugar propio de inserción en la sociedad, que es el académico[19].

8.1.2 Visión de la Universidad del Norte 2013-2022

En el año 2022, la Universidad del Norte seguirá siendo una de las mejores universidades del país, de América Latina y el Caribe, por su compromiso con la excelencia en la formación de sus estudiantes y en la creación del conocimiento, su alto impacto en el desarrollo, regional y nacional, y el diálogo con la sociedad global en la búsqueda continua de un futuro mejor.

En la realización de su Visión a 2022, la universidad fortalecerá sus acreditaciones, su posicionamiento en los rankings internacionales como reconocimiento a la excelencia en los procesos de enseñanza aprendizaje, con innovación y pedagogía, el alto nivel científico de su cuerpo profesoral y la proyección internacional de la extensión.

Incrementará y dinamizará la competitividad de sus egresados, quienes serán aliados estratégicos en la ejecución de proyectos y en el fortalecimiento de los vínculos con el sector empresarial.

8.2. ESTADO ACTUAL DEL GOBIERNO

8.2.1. Gobierno Organizacional

La Universidad del Norte tiene implementado toda una estructura de Gobierno tanto en lo institucional como en sus diferentes áreas. Su A*creditación institucional de Alta Calidad* en lo que concierne a lo académico junto a la certificación ISO 9001:2015 para sus procesos administrativos, le facilita alinear las estrategias establecidas.

[19] Misión y Visión de Uninorte. https://www.uninorte.edu.co/web/sobre-nosotros/mision-vision

En lo que concierne a Gobierno institucional, la Universidad cuenta con un Consejo Directivo que ejerce las tareas de Evaluación, Supervisión y Medición a nivel organizativo.

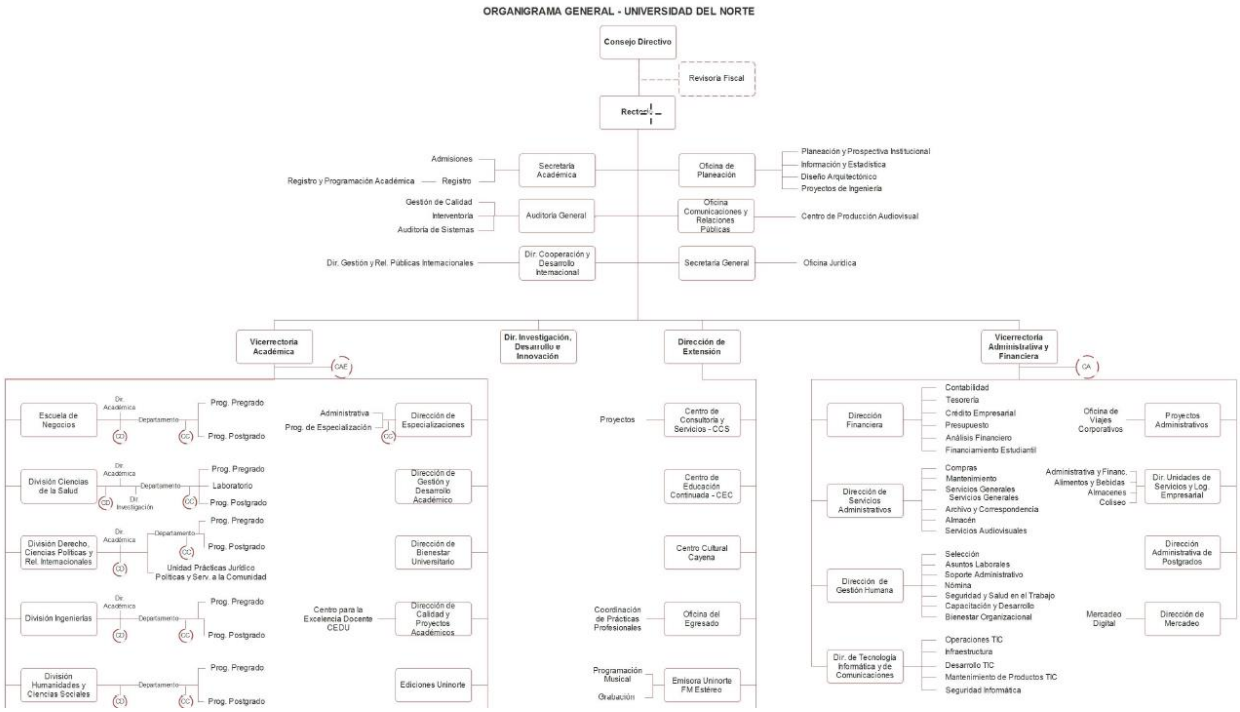

Figura 6. Organigrama de la Universidad del Norte[20].

La Universidad en su accionar tiene que cada 5 años establece un plan estratégico en el cual incluye todos los retos en los que se embarcará para lograr lo que ha visionado. En el plan establecido para el quinquenio 2018-2022, Jesús Ferro Bayona su Rector expresa: "La universidad del futuro es la que alcance la mayor integración entre el arte y la ciencia. Fortalecer, por tanto, esa universidad de las ciencias y del arte, del humanismo y de la ética, es nuestra gran labor de los años por venir: Universidad del conocimiento, en la que nos relacionamos para ser creativos y, por ese camino, transformarnos."[21]

8.2.2. Gobierno TI

El área de Tecnología Informática y de Comunicaciones tiene como visión ser el socio estratégico para el logro de los objetivos institucionales, adoptando tecnologías y

[20] Tomado de https://www.uninorte.edu.co/web/sobre-nosotros/organigrama

[21] https://www.uninorte.edu.co/documents/10698/13338003/Plan+de+Desarrollo+2018-2022+final.pdf/ea53c16f-75e6-46ec-8962-dfd1b35f8d1c

estándares de TI acordes con las tendencias mundiales, que permitan la implementación de servicios ágiles y oportunos; garantizando la calidad, seguridad y efectividad de los mismos[22].

Son funciones de la Dirección de Tecnología Informática y de Comunicaciones:

- Responder por la planeación, adquisición, actualización, implementación, operación y calidad de la infraestructura, procesos y productos relacionados con la tecnología informática y de comunicaciones; cuidando que las inversiones requeridas signifiquen un menor costo y un mayor beneficio institucional.
- Definir estrategias y procesos que garanticen la disponibilidad, confiabilidad, confidencialidad, integridad, eficiencia y eficacia de los productos TIC y de la infraestructura tecnológica sobre la cual operan.
- Participar, junto con la Vicerrectoría Administrativa y Financiera, en la definición de políticas de desarrollo y seguridad en el área de informática y comunicaciones.
- Definir planes e implementar mediciones para el aseguramiento de la calidad de los productos, servicios y procesos de la Gestión de Tecnología Informática y de Comunicaciones.
- Evaluar y aprobar la adopción de nuevas tecnologías, marcos de referencia y mejores prácticas relacionadas con la implementación, operación y soporte de los servicios de tecnología informática y de comunicaciones.

El área de Tecnología Informática y de Comunicaciones tiene implementados 5 procesos bajo las normas ISO 9001:2015 y diseñados bajo las mejores prácticas de ITIL 3.

Figura 7. Procesos del área TIC de Uninorte

[22] https://www.uninorte.edu.co/web/gestion-administrativa-y-financiera/direccion-de-tecnologia-informatica-y-de-comunicaciones

En la siguiente figura encontrará el organigrama actual de esta área.

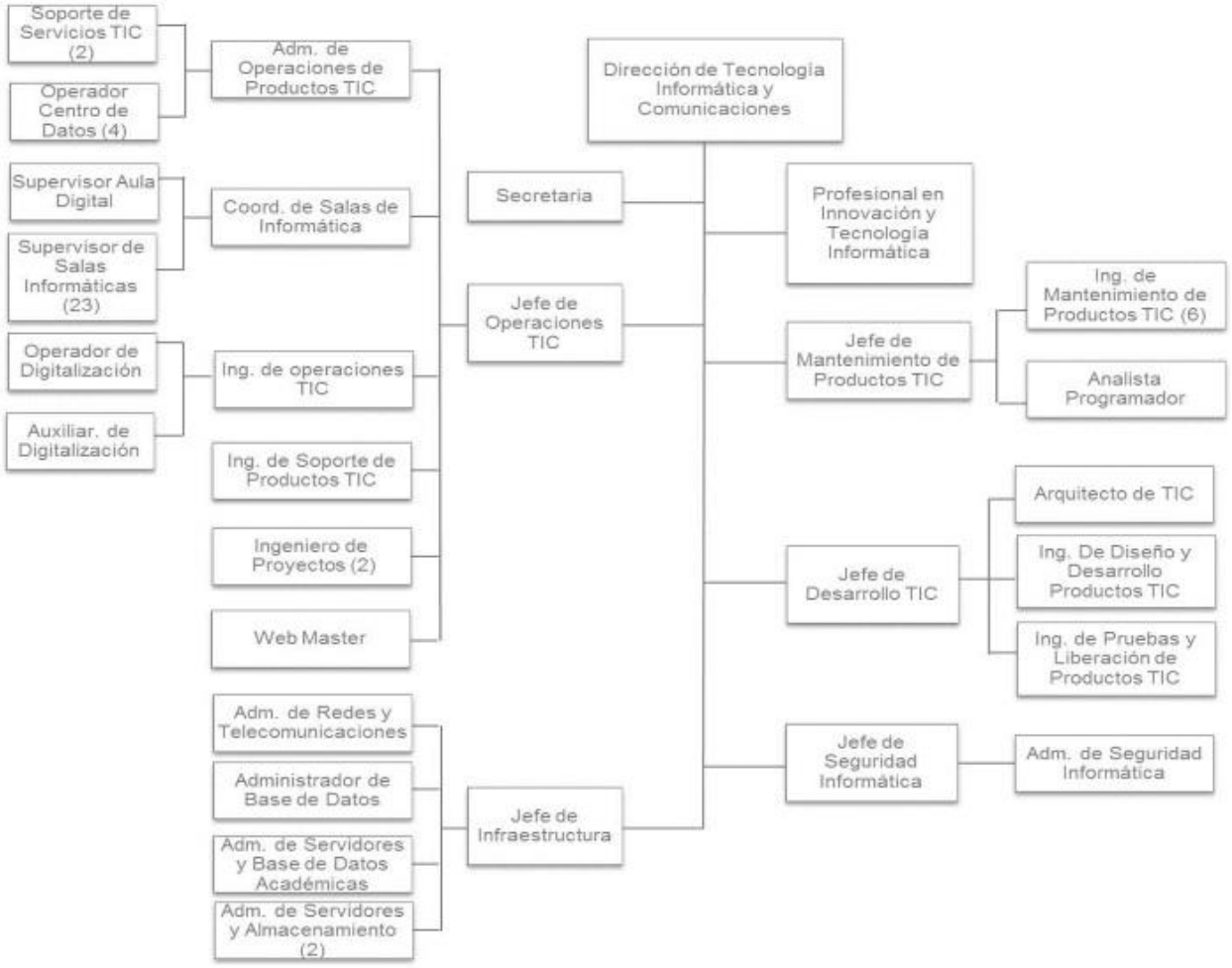

Figura 8. Organigrama de la Dirección de TI de la Universidad del Norte[23]

[23] https://www.uninorte.edu.co/web/gestion-administrativa-y-financiera/direccion-de-tecnologia-informatica-y-de-comunicaciones

8.3. EVALUACIÓN DEL PROTOCOLO GGIA EN UNINORTE

8.3.1. Medición de la Madurez inicial

Al aplicar la herramienta de medición de madurez del protocolo GGIA en la Universidad del Norte se tuvieron estos resultados. En el anexo 1 se muestra el formulario diligenciado con todas las respuestas.

Proceso	Inicial
Gestión de Política de Control de acceso	4
Gestión de Marco de Gestión de TI	3
Gestión de Estrategia	3,5
Gestión de Definición de requisitos	3
Gestión de Cambios	4
Gestión de Activos	5
Gestión de Configuración	3
Gestión de Servicios de seguridad	4
Gestión de Controles de procesos corporativos	3
Supervisar, Evaluar y Valorar Rendimiento y Conformidad	4,5
Supervisar, Evaluar y Valorar Conformidad de Req Externos	4
PROMEDIO	**3,7**

Tabla 7. Evaluación inicial Uninorte

8.3.2 Análisis de resultados y plan de mejora fase 1

Teniendo en cuenta que:

- Se hará énfasis en los procesos en los que el puntaje obtenido fue el menor (3).
- Es esencial tener una política de acceso completa.

Se propone este plan de trabajo inicial:

Actividad	Apoyo	Inicio	Fin
Implementar una política de acceso para cuentas con acceso privilegiado y personas con contrato civil. Determinar una periodicidad para la revisión de políticas	G. Humana Dir. Jurídica	07/2018	08/2018

Establecer un mecanismo que permita que los propietarios de los activos revisen de forma periódica los derechos de acceso de los usuarios	Seguridad Informática	07/2018	03/2019
Establecer un procedimiento para identificar y priorizar los requisitos funcionales, técnicos, de información y de control del GGIA de forma alineada al negocio	Arquitectura TI	07/2018	12/2018
Establecer un procedimiento para mantener un modelo lógico de los servicios, activos e infraestructura y sobre cómo registrar los ítems de configuración (CIs) y las relaciones entre ellos	Operaciones TI	07/2018	12/2018

Tabla 8. Plan inicial Uninorte

8.3.3. Medición de la Madurez al completar la fase 1 de mejoramiento

Al aplicar la herramienta de medición de madurez del protocolo GGIA en la Universidad del Norte después de ejecutada la fase 1, se tuvieron estos resultados. En el anexo 2 se muestra el formulario diligenciado con todas las respuestas.

Proceso	Ejecutada la fase 1
Gestión de Política de Control de acceso	5
Gestión de Marco de Gestión de TI	3
Gestión de Estrategia	4
Gestión de Definición de requisitos	4
Gestión de Cambios	4
Gestión de Activos	5
Gestión de Configuración	3
Gestión de Servicios de seguridad	4
Gestión de Controles de procesos corporativos	3
Supervisar, Evaluar y Valorar Rendimiento y Conformidad	4,5
Supervisar, Evaluar y Valorar Conformidad de Req Externos	4
PROMEDIO	**4,0**

Tabla 9. Evaluación luego de aplicar la fase 1 en Uninorte

Se puede notar que el nivel de madurez los procesos Gestión de la Política de Control de acceso, Gestión de la Estrategia TI y Gestión de Definición de requisitos aumentaron sus niveles de madurez.

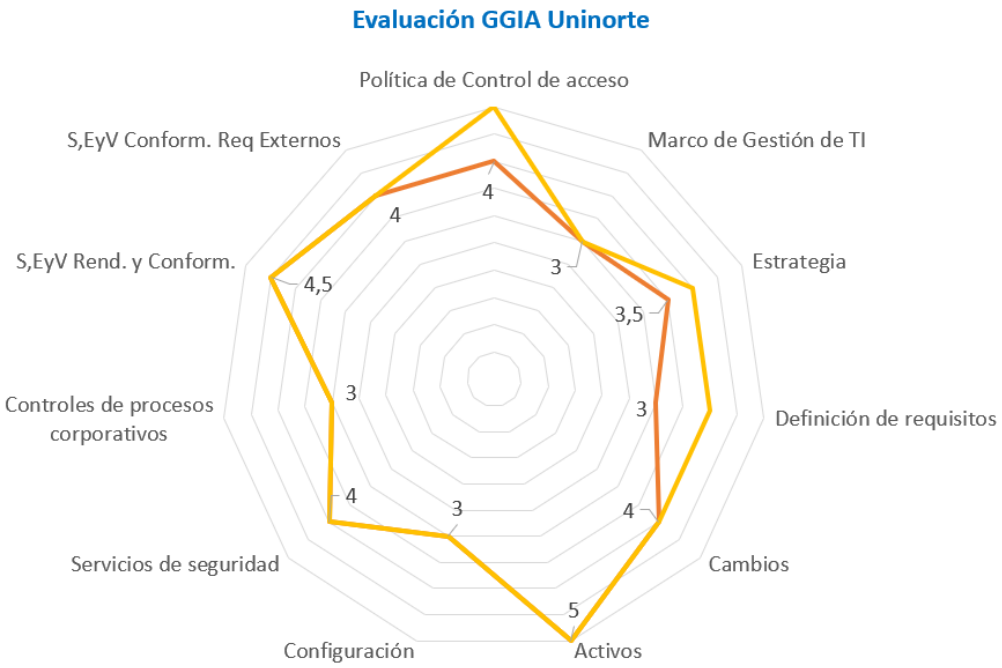

Figura 6. Variación en los niveles de madurez luego de aplicar la fase 1.

8.3.4. Análisis de resultados y plan de mejora fase 2

Teniendo en cuenta que se hará énfasis en los procesos en los que el puntaje obtenido aún es menor (3), se propone este plan de trabajo para la fase 2.

Actividad	Apoyo	Inicio	Fin
Alinear el análisis de segregación de funciones con los accesos concedidos	Auditoría	02/2019	12/2019
Establecer un procedimiento para definir y mantener responsabilidades sobre la propiedad de la información (datos) y de los sistemas	Auditoría	02/2019	12/2019
Establecer un procedimiento para crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones	Auditoría	02/2019	12/2019
Incluir las capacidades y servicios GGIA en el marco de la arquitectura empresarial	Arquitectura TI	02/2019	06/2019

Tabla 9. Plan fase 1 Uninorte

8.3.5. Medición de la Madurez al completar la fase 2 de mejoramiento

Al aplicar la herramienta de medición de madurez del protocolo GGIA en la Universidad del Norte después de ejecutada la fase 2, se tuvieron estos resultados. En el anexo 3 se muestra el formulario diligenciado con todas las respuestas.

Proceso	Ejecutada la fase 2
Gestión de Política de Control de acceso	5
Gestión de Marco de Gestión de TI	4
Gestión de Estrategia	4
Gestión de Definición de requisitos	4
Gestión de Cambios	4
Gestión de Activos	5
Gestión de Configuración	4
Gestión de Servicios de seguridad	4
Gestión de Controles de procesos corporativos	3,3
Supervisar, Evaluar y Valorar Rendimiento y Conformidad	4,5
Supervisar, Evaluar y Valorar Conformidad de Req Externos	4
PROMEDIO	**4,2**

Tabla 11. Evaluación luego de aplicar la fase 2 en Uninorte

Se puede notar que el nivel de madurez los procesos Gestión de Marco de Gestión de TI, Gestión de Configuración y Gestión de Controles de procesos corporativos aumentaron sus niveles de madurez.

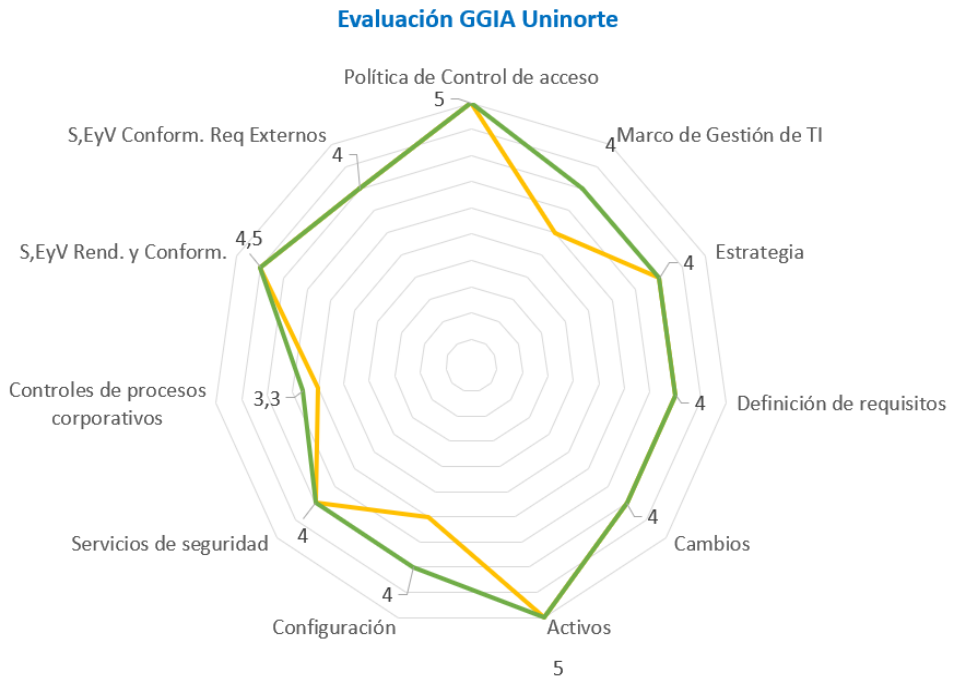

Figura 7. Variación en los niveles de madurez luego de aplicar la fase 1.

Finalmente se muestra todos los cambios en los niveles de madurez luego de aplicar la fase inicial o 1 y la final o 2.

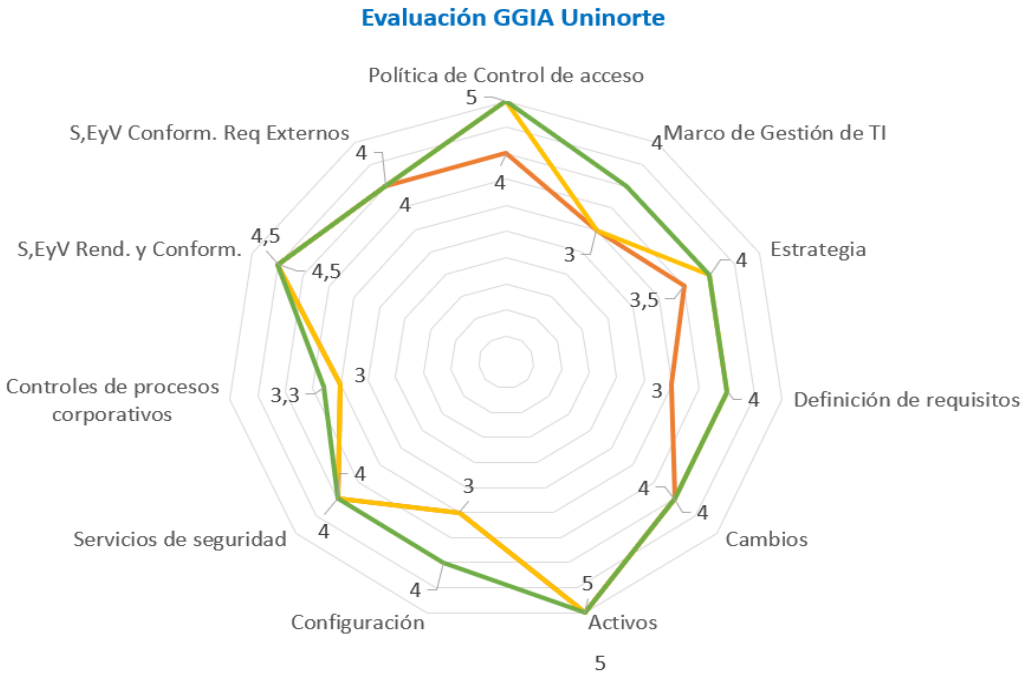

Figura 8. Variación en los niveles de madurez luego de todo el plan de mejora.

9. CONCLUSIONES

- El uso de Tecnología Informática es una Institución de Educación Superior (IES) actualmente es prácticamente obligatorio. Por ello, a su vez, se hace requerido implementar un Gobierno de TI.

- COBIT 5 provee lineamientos, objetivos, actividades y métricas entre otros, que facilitan ampliamente el definir un protocolo de Gobierno y Gestión de Identidades Digitales y de Acceso. Esto permite que en dicho ejercicio sea posible centrarse en mayor medida en la definición de las necesidades y reglas del negocio.

- ITIL provee un conjunto de buenas prácticas para la gestión de acceso que se complementan con lo que propone COBIT.

- ISO 27002 incluye en unos de sus controles (9, control de acceso) recomendaciones fundamentales para la definición de una política de gestión de acceso completa.

- Una de las grandes preocupaciones de las áreas de Tecnología de las IES es la seguridad informática. Desplegar un protocolo de Gobierno y Gestión de Identidades Digitales y Accesos es crucial para reducir riesgos en ese sentido y además aporta en la buena gestión de los recursos de la compañía, con lo que finalmente se estará aportando a cumplir con los objetivos del Gobierno Corporativo y por lo tanto, generando valor.

- Para implementar de forma exitosa una solución de Gestión de Identidades Digitales y Accesos, es esencial no solo centrarse en los requerimientos técnicos y la interacción entre las diferentes tecnologías. Antes de ello, se deben tener definido todos los aspectos de gobierno y buenas prácticas.

- Si bien la Universidad del Norte tiene un proceso implementado para el Gobierno y Gestión de Identidades Digitales y Acceso basado en ISO 9001:2015 e ITIL 3 con varios años de madurez, al aplicarle la evaluación del protocolo diseñado nos permitió identificar varios aspectos a mejorar, lo cual contribuirá en gran medida a fortalecer su Gobierno TI.

BIBLIOGRAFÍA

Arveson, P. (1998) The Deming Cycle. BSC. Recuperado de: http://www.balancedscorecard.org/BSC-Basics/Articles-Videos/The-Deming-Cycle

Bertino, E., Takahashi, K. (2010). Identity Management: Concepts, Technologies, and Systems.

Big Data Social. 2016. ¿Qué es el Cuadrante Mágico de Gartner? Recuperado de: http://www.bigdata-social.com/informe-cuadrante-magico-gartner/

Gartner. (2017). Magic Quadrant for Access Management, Worldwide.

Dolnick, D. (2017). Top 3 IAM Trends to Watch for in 2018. Recuperado de: https://www.onelogin.com/blog/top-3-iam-trends-to-watch-for-in-2018

EDUCAUSE. The EDUCAUSE Information Security Almanac. 2017. Recuperado de: https://library.educause.edu/resources/2017/5/the-educause-information-security-almanac-2017

Etges, Rafael. (2011). The Impact of Governance on Identity Management Programs. ISACA. Recuperado de: https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/The-Impact-of-Governance-on-Identity-Management-Programs.aspx

Harvard University. Identity & Access Management. Recuperado de: https://iam.harvard.edu/get-started/authentication

Iglesias, Ignacio. (2014). Por qué implantar un sistema de gestión de identidad open source: WBSVision. Recuperado de: http://www.whitebearsolutions.com/por-que-implantar-un-sistema-de-gestion-de-identidad-open-source-wbsvision/

ISACA. (2012). COBIT 5: Un marco de negocio para el gobierno y la gestión de las TI de la empresa.

ISACA. (2012). COBIT 5, Procesos Catalizadores.

ISACA. (2005). IT Governance. Developing a successful governance strategy. https://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Study-Materials/Documents/Developing-a-Successful-Governance-Strategy.pdf

ISACA. (2011). The Impact of Governance on Identity Management Programs. Etges R. ISACA. Recuperado de: https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/The-Impact-of-Governance-on-Identity-Management-Programs.aspx

ISO. (2013). ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management.

Keller, G. (2016). Protocols using Identity Management. Recuperado de: https://jumpcloud.com/blog/protocols-using-identity-management/

OGC. (2011). ITIL Service Operation.

Pettey, C. (2017). Identity and Access Management in the Digital Age. Recuperado de: https://www.gartner.com/smarterwithgartner/identity-and-access-management-in-the-digital-age/

Ross, J., & Weil, P. (2002). Six IT Decision Your IT People Shouldn't Make. Harvard Business Review. Recuperado de: http://www.qualified-audit-partners.be/user_files/ITforBoards/GVIT_Harvard_Business_Review-Ross_Jeane__Weill_Peter_Six_IT_Decsions_Your_IT_People_Shouldnt_Make_2002.pdf

SANS. (2005). Identity and Access Management Solution.

Selig, Gad & Wilkinson, Jayne. (2008). Implementing IT Governance: A Practical Guide to Global Best Practices in IT Management.

Sila Solutions Group. (2018). 2018 Trends & Predictions in Identity Management. Recuperado de: https://silasg.com/insights/2018-trends-predictions-identity-management

The Institute of Internal Auditors. (2007). Identity and Access Management. Recuperado de: https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%209%20-%20Identity%20and%20Access%20Management.pdf

Universidad del Norte. Misión de la Universidad del Norte. Recuperado de: https://www.uninorte.edu.co/documents/10698/13334705/Boletin+Estadistico+2017+Nuevoo.pdf/67355a04-6b2e-4c6b-9f0c-e8fd98045790

Valentine, B. (2017). Current Trends in Identity and Access Management: July 2017. Recuperado de: https://securityintelligence.com/current-trends-in-identity-and-access-management-july-2017/

Van Grembergen y De Haes. (2015). Enterprise Governance of Information Technology.

ANEXO 1. FORMULARIO EVALUACIÓN INICIAL UNINORTE

Proceso	Pregunta		Respuesta	Puntaje
Gestionar Política de Control de acceso	1	¿Se cuenta con una política de control de acceso con base en los requisitos del negocio y de seguridad de la información?	4	4
	2	¿En caso de contar con una polìtica, esta es revisada periódicamente?	4	
	3	¿Dicha política contempla a los funcionarios, profesores, estudiantes, egresados, proveedores, contratistas y en general toda la comunidad que requiere acceso?	4	
Gestionar el Marco de Gestión de TI	4	¿Se cuenta con un procedimiento para definir y mantener responsabilidades sobre la propiedad de la información (datos) y de los sistemas?	3	3
	5	¿Se cuenta con un procedimiento para crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones?	3	
Gestionar la Estrategia GGIA	6	¿Se evalúa el rendimiento del negocio actual, las capacidades y los servicios TI externos y se comprende la arquitectura corporativa en relación con el GGIA.?	3	3,5
	7	¿Se Identifican asuntos relevantes que hayan ocurrido y se desarrollan recomendaciones en áreas que puedan mejorar el GGIA?	4	
Gestionar la definición de requisitos GGIA	8	¿A partir de la base del modelo conceptual de negocio, se identifica, prioriza, específica y acuerdan los requisitos funcionales, técnicos, de información y de control?	3	3
Gestionar los Cambios GGIA	9	¿Se evalúan todas las peticiones de cambio GGIA para determinar el impacto en el negocio y los procesos y servicios de IT, y para evaluar si el cambio afectará de forma negativa al entorno operacional o si introducirá algún riesgo no aceptable?	4	4

	10	¿Se Asegura que los cambios son registrados, priorizados, categorizados, analizados, autorizados y planificados?	4	
Gestionar los activos GGIA	11	¿Al activar una identidad digital se tiene en cuenta que se cuente con licencias disponibles?	5	5
Gestionar la configuración GGIA	12	¿Se establece y mantiene un modelo lógico de los servicios, activos e infraestructura y sobre cómo registrar los ítems de configuración (CIs) y las relaciones entre ellos?	3	3
	13	¿Se incluyen los CIs considerados necesarios para gestionar eficazmente los servicios y proveer una descripción única y confiable de los activos de un servicio?	3	
Gestionar servicios de seguridad GGIA	14	¿Todos los usuarios tienen un único identificador y los derechos de acceso acordes con su función en la empresa??	3	4
	15	¿Se asegura que todos los usuarios tienen derechos de acceso a la información acordes con sus requisitos de negocio?	3	
	16	¿Se coordinar con las unidades par que gestionen sus propios derechos de acceso en los procesos de negocio?	4	
	17	¿Se permite únicamente el acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente?	5	
	18	¿Se cuenta con un proceso formal de registro y de cancelación de registro de usuarios que posibilita la asignación de los derechos de acceso?	4	
	19	¿Se cuenta con un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios?	4	

	20	¿Se restringe y controla la asignación y uso de cuentas de acceso privilegiado (administración, root)?	4	
	21	¿Se cuenta con un proceso formal para la asignación secreta de contraseñas?	5	
	22	¿Los propietarios de los activos revisan con una frecuencia determinada los derechos de acceso de los usuarios?	2	
	23	¿Los derechos de acceso a aplicativos o lugares de profesores, funcionarios, estudiantes, egresados o proveedores son retirados al terminar su empleo, contrato o acuerdo, o se ajustan cuando se hacen cambios?	4	
	24	¿Las contraseñas se cifran cuando son transmitidas o almacenadas?	4	
	25	¿Se cuenta con una opción que permita los usuarios recordar su identificación de acceso a los servicios TI?	5	
	26	¿Se cuenta con un metadirectorio de usuarios como LDAP o Active Directory con el fin de centralizar los usuarios?	4	
	27	¿Se cuenta con herramientas de logon ùnico como CAS, SAML, OpenID, etc con el fin de facilitar el acceso a los usuarios?	4	
	28	¿Se cuenta con una solución de gestión de identidades que facilita la automatización de las políticas establecidas?	3	
	29	¿Se cuenta con una opción que permite a los usuarios reasignar de forma segura su contraseña en caso de olvido?	5	
Gestionar controles de procesos corporativos	30	¿El inventario de funciones, responsabilidades y derechos de acceso está alineado con las necesidades de negocio autorizadas?	4	3

	31	¿Se administran las funciones de negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de proceso del negocio?	2	
	32	¿Se gestiona la autorización al acceso a los recursos de información relacionados con los procesos de información, incluyendo los custodiados por la empresa, por TI y por terceros?	3	
Supervisar, Evaluar y Valorar Rendimiento y Conformidad GIA	33	¿Se involucran a las partes interesadas y se comunican los objetivos y requisitos del proceso?	4	4,5
	34	¿Se tienen definidos objetivos, métricas y la retención de datos (evidencias)?	5	
Supervisar, Evaluar y Valorar la Conformidad GIA con los Requerimientos Externos	35	¿Se identifican y valoran la totalidad de los posibles requisitos de cumplimiento y su impacto sobre las actividades de GGIA en ámbitos como los flujos de datos, la privacidad, los controles internos, los informes financieros, la regulación sectorial, la propiedad intelectual y la seguridad e higiene en el trabajo?	4	4

ANEXO 2. FORMULARIO EVALUACIÓN AL EJECUTAR LA FASE 1 EN UNINORTE

Proceso		Pregunta	Respuesta	Puntaje
Gestionar Política de Control de acceso	1	¿Se cuenta con una política de control de acceso con base en los requisitos del negocio y de seguridad de la información?	5	5
	2	¿En caso de contar con una polìtica, esta es revisada periódicamente?	5	
	3	¿Dicha política contempla a los funcionarios, profesores, estudiantes, egresados, proveedores, contratistas y en general toda la comunidad que requiere acceso?	5	
Gestionar el Marco de Gestión de TI	4	¿Se cuenta con un procedimiento para definir y mantener responsabilidades sobre la propiedad de la información (datos) y de los sistemas?	3	3
	5	¿Se cuenta con un procedimiento para crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones?	3	
Gestionar la Estrategia GGIA	6	¿Se evalúa el rendimiento del negocio actual, las capacidades y los servicios TI externos y se comprende la arquitectura corporativa en relación con el GGIA.?	4	4
	7	¿Se Identifican asuntos relevantes que hayan ocurrido y se desarrollan recomendaciones en áreas que puedan mejorar el GGIA?	4	
Gestionar la definición de requisitos GGIA	8	¿A partir de la base del modelo conceptual de negocio, se identifica, prioriza, específica y acuerdan los requisitos funcionales, técnicos, de información y de control?	4	4
Gestionar los Cambios GGIA	9	¿Se evalúan todas las peticiones de cambio GGIA para determinar el impacto en el negocio y los procesos y servicios de IT, y para evaluar si el cambio afectará de forma negativa al entorno operacional o si introducirá algún riesgo no aceptable?	4	4

	10	¿Se Asegura que los cambios son registrados, priorizados, categorizados, analizados, autorizados y planificados?	4	
Gestionar los activos GGIA	11	¿Al activar una identidad digital se tiene en cuenta que se cuente con licencias disponibles?	5	5
Gestionar la configuración GGIA	12	¿Se establece y mantiene un modelo lógico de los servicios, activos e infraestructura y sobre cómo registrar los ítems de configuración (CIs) y las relaciones entre ellos?	3	3
	13	¿Se incluyen los CIs considerados necesarios para gestionar eficazmente los servicios y proveer una descripción única y confiable de los activos de un servicio?	3	
Gestionar servicios de seguridad GGIA	14	¿Todos los usuarios tienen un único identificador y los derechos de acceso acordes con su función en la empresa??	3	4
	15	¿Se asegura que todos los usuarios tienen derechos de acceso a la información acordes con sus requisitos de negocio?	3	
	16	¿Se coordinar con las unidades par que gestionen sus propios derechos de acceso en los procesos de negocio?	4	
	17	¿Se permite únicamente el acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente?	5	
	18	¿Se cuenta con un proceso formal de registro y de cancelación de registro de usuarios que posibilita la asignación de los derechos de acceso?	4	
	19	¿Se cuenta con un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios?	4	
	20	¿Se restringe y controla la asignación y uso de cuentas de acceso privilegiado (administración, root)?	4	

	21	¿Se cuenta con un proceso formal para la asignación secreta de contraseñas?	5	
	22	¿Los propietarios de los activos revisan con una frecuencia determinada los derechos de acceso de los usuarios?	4	
	23	¿Los derechos de acceso a aplicativos o lugares de profesores, funcionarios, estudiantes, egresados o proveedores son retirados al terminar su empleo, contrato o acuerdo, o se ajustan cuando se hacen cambios?	4	
	24	¿Las contraseñas se cifran cuando son transmitidas o almacenadas?	4	
	25	¿Se cuenta con una opción que permita los usuarios recordar su identificación de acceso a los servicios TI?	5	
	26	¿Se cuenta con un metadirectorio de usuarios como LDAP o Active Directory con el fin de centralizar los usuarios?	4	
	27	¿Se cuenta con herramientas de logon ùnico como CAS, SAML, OpenID, etc con el fin de facilitar el acceso a los usuarios?	4	
	28	¿Se cuenta con una solución de gestión de identidades que facilita la automatización de las políticas establecidas?	3	
	29	¿Se cuenta con una opción que permite a los usuarios reasignar de forma segura su contraseña en caso de olvido?	5	
Gestionar controles de procesos corporativos	30	¿El inventario de funciones, responsabilidades y derechos de acceso está alineado con las necesidades de negocio autorizadas?	4	3,0
	31	¿Se administran las funciones de negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de proceso del negocio?	2	

	32	¿Se gestiona la autorización al acceso a los recursos de información relacionados con los procesos de información, incluyendo los custodiados por la empresa, por TI y por terceros?	3	
Supervisar, Evaluar y Valorar Rendimiento y Conformidad GIA	33	¿Se involucran a las partes interesadas y se comunican los objetivos y requisitos del proceso?	4	4,5
	34	¿Se tienen definidos objetivos, métricas y la retención de datos (evidencias)?	5	
Supervisar, Evaluar y Valorar la Conformidad GIA con los Requerimientos Externos	35	¿Se identifican y valoran la totalidad de los posibles requisitos de cumplimiento y su impacto sobre las actividades de GGIA en ámbitos como los flujos de datos, la privacidad, los controles internos, los informes financieros, la regulación sectorial, la propiedad intelectual y la seguridad e higiene en el trabajo?	4	4

ANEXO 3. FORMULARIO EVALUACIÓN AL EJECUTAR LA FASE 2 EN UNINORTE

Proceso	Pregunta		Respuesta	Puntaje
Gestionar Política de Control de acceso	1	¿Se cuenta con una política de control de acceso con base en los requisitos del negocio y de seguridad de la información?	5	5
	2	¿En caso de contar con una polìtica, esta es revisada periódicamente?	5	
	3	¿Dicha política contempla a los funcionarios, profesores, estudiantes, egresados, proveedores, contratistas y en general toda la comunidad que requiere acceso?	5	
Gestionar el Marco de Gestión de TI	4	¿Se cuenta con un procedimiento para definir y mantener responsabilidades sobre la propiedad de la información (datos) y de los sistemas?	4	4
	5	¿Se cuenta con un procedimiento para crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones?	4	
Gestionar la Estrategia GGIA	6	¿Se evalúa el rendimiento del negocio actual, las capacidades y los servicios TI externos y se comprende la arquitectura corporativa en relación con el GGIA.?	4	4
	7	¿Se Identifican asuntos relevantes que hayan ocurrido y se desarrollan recomendaciones en áreas que puedan mejorar el GGIA?	4	
Gestionar la definición de requisitos GGIA	8	¿A partir de la base del modelo conceptual de negocio, se identifica, prioriza, específica y acuerdan los requisitos funcionales, técnicos, de información y de control?	4	4
Gestionar los Cambios GGIA	9	¿Se evalúan todas las peticiones de cambio GGIA para determinar el impacto en el negocio y los procesos y servicios de IT, y para evaluar si el cambio afectará de forma negativa al entorno operacional o si introducirá algún riesgo no aceptable?	4	4

	10	¿Se Asegura que los cambios son registrados, priorizados, categorizados, analizados, autorizados y planificados?	4	
Gestionar los activos GGIA	11	¿Al activar una identidad digital se tiene en cuenta que se cuente con licencias disponibles?	5	5
Gestionar la configuración GGIA	12	¿Se establece y mantiene un modelo lógico de los servicios, activos e infraestructura y sobre cómo registrar los ítems de configuración (CIs) y las relaciones entre ellos?	4	4
	13	¿Se incluyen los CIs considerados necesarios para gestionar eficazmente los servicios y proveer una descripción única y confiable de los activos de un servicio?	4	
Gestionar servicios de seguridad GGIA	14	¿Todos los usuarios tienen un único identificador y los derechos de acceso acordes con su función en la empresa.?	3	4
	15	¿Se asegura que todos los usuarios tienen derechos de acceso a la información acordes con sus requisitos de negocio?	3	
	16	¿Se coordinar con las unidades par que gestionen sus propios derechos de acceso en los procesos de negocio?	4	
	17	¿Se permite únicamente el acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente?	5	
	18	¿Se cuenta con un proceso formal de registro y de cancelación de registro de usuarios que posibilita la asignación de los derechos de acceso?	4	
	19	¿Se cuenta con un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios?	4	
	20	¿Se restringe y controla la asignación y uso de cuentas de acceso privilegiado (administración, root)?	4	

	21	¿Se cuenta con un proceso formal para la asignación secreta de contraseñas?	5	
	22	¿Los propietarios de los activos revisan con una frecuencia determinada los derechos de acceso de los usuarios?	4	
	23	¿Los derechos de acceso a aplicativos o lugares de profesores, funcionarios, estudiantes, egresados o proveedores son retirados al terminar su empleo, contrato o acuerdo, o se ajustan cuando se hacen cambios?	4	
	24	¿Las contraseñas se cifran cuando son transmitidas o almacenadas?	4	
	25	¿Se cuenta con una opción que permita los usuarios recordar su identificación de acceso a los servicios TI?	5	
	26	¿Se cuenta con un metadirectorio de usuarios como LDAP o Active Directory con el fin de centralizar los usuarios?	4	
	27	¿Se cuenta con herramientas de logon ùnico como CAS, SAML, OpenID, etc con el fin de facilitar el acceso a los usuarios?	4	
	28	¿Se cuenta con una solución de gestión de identidades que facilita la automatización de las políticas establecidas?	3	
	29	¿Se cuenta con una opción que permite a los usuarios reasignar de forma segura su contraseña en caso de olvido?	5	
Gestionar controles de procesos corporativos	30	¿El inventario de funciones, responsabilidades y derechos de acceso está alineado con las necesidades de negocio autorizadas?	4	3,3
	31	¿Se administran las funciones de negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de proceso del negocio?	3	

	32	¿Se gestiona la autorización al acceso a los recursos de información relacionados con los procesos de información, incluyendo los custodiados por la empresa, por TI y por terceros?	3	
Supervisar, Evaluar y Valorar Rendimiento y Conformidad GIA	33	¿Se involucran a las partes interesadas y se comunican los objetivos y requisitos del proceso?	4	4,5
	34	¿Se tienen definidos objetivos, métricas y la retención de datos (evidencias)?	5	
Supervisar, Evaluar y Valorar la Conformidad GIA con los Requerimientos Externos	35	¿Se identifican y valoran la totalidad de los posibles requisitos de cumplimiento y su impacto sobre las actividades de GGIA en ámbitos como los flujos de datos, la privacidad, los controles internos, los informes financieros, la regulación sectorial, la propiedad intelectual y la seguridad e higiene en el trabajo?	4	4